

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-169272

(43)Date of publication of application : 23.06.1998

(51)Int.Cl.

E05B 49/00

G01S 13/75

G01S 13/76

G01S 13/79

(21)Application number : 08-352328

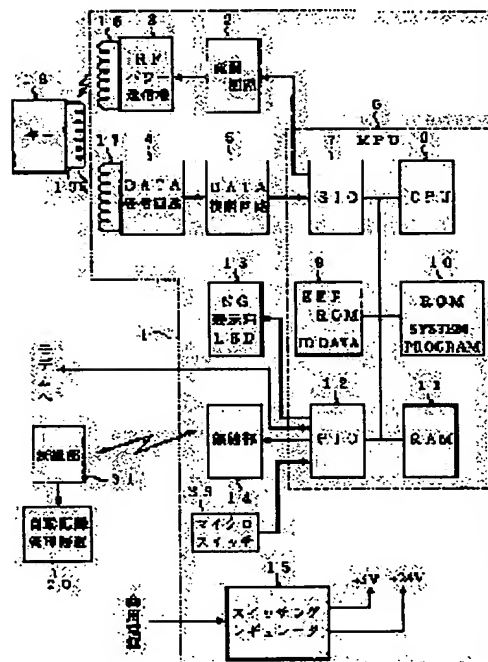
(71)Applicant : UNITEC KK  
TAKIGEN MFG CO LTD

(22)Date of filing : 12.12.1996

(72)Inventor : SASAKI KAZUO  
HIRANO MASAMI**(54) LOCK CONTROL SYSTEM****(57)Abstract:**

**PROBLEM TO BE SOLVED:** To provide a control system capable of easily controlling entering and exiting, maintenance, and the like.

**SOLUTION:** A reader 1 on a storage shed normally transmits RF power signals at predetermined time intervals. When an operator inserts a key provided with a transponder 18 into a keyhole, a system is operated on receiving the RF power signal, and transmits ID data stored in an EEPROM. The reader 1 receives the ID data and compares it with ID data preset in the EEPROM 9, and when they are coincident, stores key ID data (whether separate or master) for identifying the time and date when unlocking has been done and a transponder (key or card) used for unlocking, as system operation data. The system operation data is periodically transmitted from the radio-transmitting part 14 of the reader 1, is received by the radio-receiving part 31 of an automatic record control device 20, and is summed or printed for output in a predetermined format.

**LEGAL STATUS**

[Date of request for examination]

02.12.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-169272

(43) 公開日 平成10年(1998) 6月23日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

E 0 5 B 49/00

E 0 5 B 49/00

K

G 0 1 S 13/75

G 0 1 S 13/80

13/76

13/79

審査請求 未請求 請求項の数12 F D (全 17 頁)

(21) 出願番号 特願平8-352328

(22) 出願日 平成8年(1996)12月12日

(71) 出願人 391030538

ユニテック株式会社

東京都大田区中央2丁目25番6号

(71) 出願人 000108708

タキゲン製造株式会社

東京都品川区西五反田1丁目24番4号

(72) 発明者 佐々木 和夫

東京都大田区中央2丁目25番6号 ユニテック株式会社内

(72) 発明者 平野 正己

東京都大田区中央2丁目25番6号 ユニテック株式会社内

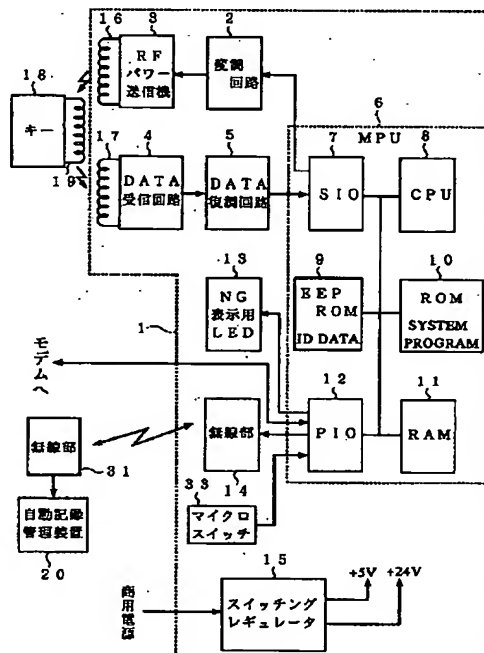
(74) 代理人 弁理士 鹿嶋 英資

(54) 【発明の名称】 錠開閉管理システム

(57) 【要約】

【課題】 入退室やメンテナンス等を容易に管理することができる錠開閉管理システムを提供する。

【解決手段】 保管庫のリーダ1では、通常、RFパワー信号を所定時間間隔で送信する。これに対して、作業者がトランスポンダ18が設けられた鍵を鍵穴に挿入すると、上記RFパワー信号を受信することで作動し、EEPROM24に記憶されているIDデータを送信する。リーダ1は、上記IDデータを受信し、EEPROM9に予め設定されているIDデータと比較し、一致すると、システム運用データとして、解錠した日時、解錠に用いられたトランスポンダ(鍵またはカード)18を識別するための鍵IDデータ(個別かマスタか)を記録する。該システム運用データは、定期的にリーダ1の無線部14から送信され、自動記録管理装置20の無線部31により受信されて集計されたり、所定のフォーマットで印字出力される。



## 【特許請求の範囲】

【請求項 1】 外部の高周波磁界を各部を駆動するための電力とする装置であって、当該装置を識別するための応答装置識別データを記憶する第 1 の記憶手段および電力が印加されると前記第 1 の記憶手段に記憶されている応答装置識別データを送信する第 1 の送信手段を備え、作業者が携帯する鍵に設けられる応答装置と、前記高周波磁界を発生する高周波発生手段、前記第 1 の送信手段から送信された応答装置識別データを受信する第 1 の受信手段、当該装置に対応する応答装置を特定する応答装置識別データを記憶する第 2 の記憶手段、時刻を計時する計時手段、前記第 1 の受信手段によって受信された応答装置識別データと前記第 2 の記憶手段に記憶されている応答装置識別データとが一致した場合には、少なくとも、前記計時手段による現在時刻を記録する記録手段を備え、前記鍵によって施錠・解錠される錠側に設けられる読み取り装置とを具備することを特徴とする錠開閉管理システム。

【請求項 2】 前記読み取り装置は、前記第 1 受信手段によって受信された応答装置識別データと前記第 2 の記憶手段に記憶されている応答装置識別データとが一致しない場合、警告を発する警告手段を具備することを特徴とする請求項 1 記載の錠開閉管理システム。

【請求項 3】 前記読み取り装置は、前記高周波発生手段によって、所定時間間隔で、高周波磁界を発生することを特徴とする請求項 1 または 2 記載の錠開閉管理システム。

【請求項 4】 前記応答装置および前記読み取り装置は、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび錠の設置地域を識別するマスタ・キー・グループ識別データを授受することを特徴とする請求項 1 ないし 3 記載の錠開閉管理システム。

【請求項 5】 前記応答装置は、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第 2 の制御手段を備え、前記応答装置および前記読み取り装置は、前記所定の通信プロトコルに従って、前記システム識別データ、前記マスタ・キー・グループ識別データおよび前記応答装置識別データを授受することを特徴とする請求項 1 ないし 4 記載の錠開閉管理システム。

【請求項 6】 前記読み取り装置は、前記応答装置に対してデータを送信する第 2 の送信手段と、前記応答装置識別データの受信後、新たな応答装置識別データを生成する応答装置識別データ生成手段と、前記第 2 の記憶手段に記憶されている応答装置識別データを、前記応答装置識別データ生成手段によって生成された新たな応答装置識別データで書き換える第 1 の更新手段とを備え、前記第 2 の送信手段によって前記新たな応答装置識別データを前記応答装置に対して送信し、前記応答装置は、前記読み取り装置が送信するデータを

受信する第 2 の受信手段と、前記第 1 の記憶手段に記憶されている応答装置識別データを、前記第 2 の受信手段によって受信した前記新たな応答装置識別データで書き換える第 2 の更新手段とを備えることを特徴とする請求項 1 ないし 5 記載の錠開閉管理システム。

【請求項 7】 前記応答装置識別データおよびマスタ・キー・グループ識別データは、外部設定装置により無線通信により書換可能であることを特徴とする請求項 1 ないし 6 記載の錠開閉管理システム。

【請求項 8】 前記読み取り手段は、前記記録手段に記憶された情報を外部機器に送出する出力手段を備え、前記外部機器として、前記出力手段から出力される情報を受信する受信手段、および前記受信手段により受信した情報を集計する集計手段を備える管理手段を具備することを特徴とする請求項 1 ないし 7 記載の錠開閉管理システム。

【請求項 9】 前記出力手段は、前記記録手段に記憶された情報を無線により送信することを特徴とする請求項 8 記載の錠開閉管理システム。

【請求項 10】 前記出力手段は、前記記録手段に記憶された情報を有線により送信することを特徴とする請求項 8 記載の錠開閉管理システム。

【請求項 11】 前記出力手段は、前記記録手段に記憶された情報を電話回線を介して送信することを特徴とする請求項 8 記載の錠開閉管理システム。

【請求項 12】 前記読み取り装置は、前記錠を解錠／施錠することにより開閉される扉の開閉を検知する検出手段を具備することを特徴とする請求項 1 記載の錠開閉管理システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、入退室管理や自動販売機等のサービス管理を自動的に行う錠開閉管理システムに関する。

## 【0002】

【従来の技術】従来より、入退室する人間、入退室する時刻を制限するような施設での入退室管理においては、入退室する扉の錠を開けて入退室する際に、誰がいつ出入りしたかを、タイムレコーダ等で時刻を記録したり、入出者にサインをさせるとして行っていた。また、例えば薬剤や現金、商品等を保管する保管庫や、商品を無人で販売する自動販売機等に係るサービス管理においては、誰がいつメンテナンスを行ったかを（品物の搬入・搬出、売上回収や商品の入れ替え、補充等のために錠を開けたかを）、ノートに記帳したりするなどして行っていた。また、いずれの場合であっても、定期的に上記記録をマニュアルで集計するなどして総合的な管理を行っていた。

## 【0003】

【発明が解決しようとする課題】しかしながら、従来の

入退室管理システムやサービス管理システムでは、入退室の時刻や記名、集計などをマニュアルで行っていたため、記録を忘れたり、集計に時間や手間がかかるという問題があった。

【0004】そこで本発明は、入退室やメンテナンス時に生じる、錠の開閉を把握することにより、入退室やメンテナンス等を容易に管理することができる錠開閉管理システムを提供することを目的とする。

【0005】

【課題を解決するための手段】上記目的達成のため、請求項1記載の発明による錠開閉管理システムは、外部の高周波磁界を各部を駆動するための電力とする装置であって、当該装置を識別するための応答装置識別データを記憶する第1の記憶手段および電力が印加されると前記第1の記憶手段に記憶されている応答装置識別データを送信する第1の送信手段を備え、作業者が携帯する鍵に設けられる応答装置と、前記高周波磁界を発生する高周波発生手段、前記第1の送信手段から送信された応答装置識別データを受信する第1の受信手段、当該装置に対応する応答装置を特定する応答装置識別データを記憶する第2の記憶手段、時刻を計時する計時手段、前記第1の受信手段によって受信された応答装置識別データと前記第2の記憶手段に記憶されている応答装置識別データとが一致した場合には、少なくとも、前記計時手段による現在時刻を記録する記録手段を備え、前記鍵によって施錠・解錠される錠側に設けられる読み取り装置とを具備することを特徴とする。

【0006】また、好ましい態様として、前記読み取り装置は、例えば請求項2記載のように、前記第1受信手段によって受信された応答装置識別データと前記第2の記憶手段に記憶されている応答装置識別データとが一致しない場合、警告を発する警告手段を具備するようにしてもよい。

【0007】また、好ましい態様として、前記読み取り装置は、例えば請求項3記載のように、前記高周波発生手段によって、所定時間間隔で、高周波磁界を発生することようにしてもよい。

【0008】また、好ましい態様として、前記応答装置および前記読み取り装置は、例えば請求項4記載のように、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび特装車の設置地域を識別するマスタ・キー・グループ識別データを授受するようにしてもよい。

【0009】また、好ましい態様として、前記応答装置は、例えば請求項5記載のように、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第2の制御手段を備え、前記応答装置および前記読み取り装置は、前記所定の通信プロトコルに従って、前記システム識別データ、前記マスタ・キー・グループ識別データおよび前記応答装置識別データを授受

するようにしてもよい。

【0010】また、好ましい態様として、前記読み取り装置は、例えば請求項6記載のように、前記読み取り装置は、前記応答装置に対してデータを送信する第2の送信手段と、前記応答装置識別データの受信後、新たな応答装置識別データを生成する応答装置識別データ生成手段と、前記第2の記憶手段に記憶されている応答装置識別データを、前記応答装置識別データ生成手段によって生成された新たな応答装置識別データで書き換える第1の更新手段とを備え、前記第2の送信手段によって前記新たな応答装置識別データを前記応答装置に対して送信し、前記応答装置は、前記読み取り装置が送信するデータを受信する第2の受信手段と、前記第1の記憶手段に記憶されている応答装置識別データを、前記第2の受信手段によって受信した前記新たな応答装置識別データで書き換える第2の更新手段とを備えるようにしてもよい。

【0011】また、好ましい態様として、前記応答装置識別データおよびマスタ・キー・グループ識別データは、例えば請求項7記載のように、外部設定装置により無線通信により書換可能であってもよい。

【0012】また、好ましい態様として、前記読み取り手段は、例えば請求項8記載のように、前記記録手段に記憶された情報を外部機器に送出する出力手段を備え、前記外部機器として、前記出力手段から出力される情報を受信する受信手段、および前記受信手段により受信した情報を集計する集計手段を備える管理手段を具備するようにしてもよい。

【0013】また、好ましい態様として、前記出力手段は、例えば請求項9記載のように、前記記録手段に記憶された情報を無線により送信するようにしてもよい。

【0014】また、好ましい態様として、前記出力手段は、例えば請求項10記載のように、前記記録手段に記憶された情報を有線により送信するようにしてもよい。

【0015】また、好ましい態様として、前記出力手段は、例えば請求項11記載のように、前記記録手段に記憶された情報を電話回線を介して送信するようにしてもよい。

【0016】また、好ましい態様として、前記読み取り装置は、例えば請求項12記載のように、前記錠を解錠／施錠することにより開閉される扉の開閉を検知する検出手段を具備するようにしてもよい。

【0017】

【発明の実施の形態】以下、本発明の実施の形態を、保管庫の錠開閉管理に適用した一実施例として、図面を参照して説明する。

A. 実施例の構成

A-1. リードおよび鍵（トランスポンダ）の構成

図1は本発明の実施例による保管庫に設けられるリードおよび保管庫の錠に設けられたトランスポンダの構成を

示すブロック図である。また、図3は、上記トランスポンダのより詳細な構成例を示すブロック図である。図において、リーダ1は、既存の保管庫に設けられ、変調回路2、RFパワー送信機3、DATA受信回路4、DATA復調回路5、MPU6、NG表示用LED13、リレー14、スイッチングレギュレータ15等から構成されている。以下、各部について説明する。

【0018】変調回路2は、所定の信号を125KHzでFSK変調し、RFパワー送信機3に供給する。RFパワー送信機3は、上記変調信号をアンテナ16より送信する。上記信号としては、鍵に内蔵されている後述するトランスポンダ18を作動させるためのRFパワーや、トランスポンダ18に対して各種ID送信を要求するためのコマンドがある。次に、DATA受信回路4は、後述するトランスポンダ18から送信される、62.5KHzでPSK変調された信号をアンテナ17で受信し、DATA復調回路5に供給する。DATA復調回路5は、受信信号を復調し、データ(各種ID)を取り出し、MPU6のSIO(シリアル入出力インターフェース)7へ供給する。

【0019】MPU6は、上記SIO7、CPU(中央処理装置)8、EEPROM9、ROM(リードオンリメモリ)10、RAM(ランダムアクセスメモリ)11およびPIO(パラレル入出力インターフェース)12から構成されている。SIO7は、上記DATA復調回路5からのデータをCPU8に供給する。CPU8は、ROM10に格納されているプログラムを実行し、各種コマンドの送信、トランスポンダ18からの各種データの受信、トランスポンダ18の認証、トランスポンダ18からの各種IDデータの記録、現在時刻の計時等の制御を行う。

【0020】EEPROM9には、保管庫に設けられた当該リーダ1に対応するトランスポンダ18を識別するための各種IDデータが記憶されている。言い換えると、本リーダ1は、該EEPROM9に記憶されているIDデータに一致するIDデータを送信するトランスポンダ18が近接した場合、すなわち、保管庫に保管されている品物を搬出したり、搬入するために作業者が、対応する鍵を鍵穴に差し込んだ際、トランスポンダ18のIDデータとEEPROM9に記憶されているIDデータとが一致すると、そのときの日時やIDデータを記録するようになっている。

【0021】また、ROM10には、上述したように、CPU8によって実行されるプログラムが格納されている。RAM11は、上記CPU8の制御に伴って生成されるデータが格納されたり、ワーキングエリアとして用いられる。PIO12は、CPU8の制御の下、CPU8から供給される表示データをNG表示用LED13に供給するとともに、所定タイミングで、錠の開閉(入退室)日時やトランスポンダ18のIDデータを無線部1

4に供給する。

【0022】NG表示用LED13は、トランスポンダ18から送信されるIDデータが上記EEPROM9に格納されているIDデータと不一致である場合、すなわち、適合しない鍵で解錠されようとした場合に、点灯される表示部である。無線部14は、所定タイミングで錠の開閉(入退室)日時やトランスポンダ18のIDデータを、後述する自動記録管理システムに送信するようになっている。スイッチングレギュレータ15は、図示しない商用電源を整流し、直流電圧として、+5V、+24Vを発生し、上述した各部へ電源として供給する。

【0023】また、自動記録管理装置20は、所定の管理プログラムが実行される端末(パーソナルコンピュータ、ワークステーション等)から構成されており、上記リーダ1の無線部14から送信される錠の開閉(入退室)日時やトランスポンダ18のIDデータを無線部27で受信し、所定のフォーマットでプリンタ28で印字出力する。なお、図示の例では、リーダ1は1つしかないが、実際には、各所に設置された複数のリーダ1からの情報を受信し、一括して管理できるようになっている。

#### 【0024】A-2. 保管庫の外観構成

図2は、上述したリーダが内蔵された保管庫の外観構成を示す斜視図である。本実施例では、トランスポンダ18は、既存の鍵の把持部に埋め込まれており、保管庫に配設したリーダ1から送信されるRFパワー信号を電源として作動するようになっている。リーダ1は、常時あるいは所定時間間隔で、RFパワー信号を送信し、トランスポンダ18からの応答をチェックし、応答がなければ、何もせず、応答があれば、IDデータの認証を行うようになっている。

#### 【0025】A-3. トランスポンダの構成

図3(a)、(b)は、上述したトランスポンダ18の構成例を示すブロック図である。図3(a)に示すトランスポンダ18は、アンテナ19、送受信回路22、CPU23、EEPROM24から構成されている。アンテナ19は、上述したリーダ1から送信されるRFパワー信号や変調信号を受信し、送受信回路22に供給する。送受信回路22は、図示しない整流回路を備えており、受信したRFパワー信号を整流して所定の直流電圧を取り出し、CPU23およびEEPROM24に電源として供給するとともに、受信信号を復調し、リーダ1から送信される各種コマンドを取り出してCPU23に供給する。

【0026】CPU23は、プログラムを内蔵するROMやワークエリアとしてのRAM等を内蔵しており(図示略)、RFパワー信号により作動し、リーダ1から送信される各種コマンドを解釈し、受信したコマンドに応じて、EEPROM24に予め格納されている各種IDデータを読み出し、送受信回路22によって変調してア

ンテナ19から送信する。EEPROM24には、上述したように、予め各種IDデータが記憶されており、該各種IDデータは、CPU23によって適宜読み出される。このように、図3(a)に示すトランスポンダ18を採用した場合には、トランスポンダ18は、リーダ1からのIDデータ要求コマンドに応じて、対応するIDデータを送信する。

【0027】ここで、図4は、上記リーダ1と上記トランスポンダ18とで授受されるデータフォーマットを示す概念図である。図示するように、データは、スタートビット、データ(12ビット)、パリティビット、ストップビットから構成されており、1キャラクタ単位で、データ部分で各種IDデータを送信し、その後エラーチェック用のデータを同一フォーマットで1キャラクタ送信する。この場合、トランスポンダ18は、図5に示すように、リーダ1からの要求に応じて、システム識別IDデータ、マスターキーグループIDデータおよび鍵IDデータを送信するようになっている。すなわち、トランスポンダ18は、リーダ1からRFパワーを受信すると、まず、自動的に、システム識別IDデータを送信し、次いで、マスターキーグループID要求コマンドを受信すると、これに応じて、マスターキーグループIDデータを送信し、さらに、鍵ID要求コマンドを受信すると、これに応じて、鍵IDデータを送信する。

【0028】なお、システム識別IDデータは、例えば、特装車のメーカ毎に設定され、該メーカを識別するためのIDデータであり、固定値となっている。また、マスター・キー・グループIDデータは、保管庫の設置場所でグループ化し、該グループを識別するためのIDデータであり、変更可能となっている。さらに、鍵IDデータは、トランスポンダ(鍵)18を識別するためのIDデータであり、やはり変更可能となっている。

【0029】一方、図3(b)に示すトランスポンダ18は、アンテナ19、送受信回路26およびEEPROM27から構成されている。アンテナ19は、上述したリーダ1から送信されるRFパワー信号や変調信号を受信し、送受信回路26に供給する。送受信回路26は、図示しない整流回路を備えており、受信したRFパワー信号を整流して所定の直流電圧を取り出し、EEPROM27に電源として供給するとともに、EEPROM27から供給される各種IDデータを変調し、アンテナ19から送信する。EEPROM27には、上述したように、予め各種IDデータが記憶されており、電源が供給されると、記憶されていた各種IDデータを自動的に送受信回路26に供給する。このように、図3(b)に示すトランスポンダ18を採用した場合には、トランスポンダ18は、RFパワー信号を受信した時点で、EEPROM26に予め記憶されている各種IDデータを送信する。

【0030】ここで、図6は、上記リーダと上記トラン

スポンダとで授受されるデータフォーマットを示す概念図である。図示するように、データは、スタートビット(8ビット)、システム識別IDデータ(16ビット)、マスターキーグループIDデータ(24ビット)、鍵IDデータ(24ビット)、データBCC(16ビット)、ストップビット(8ビット)の全128ビットから構成されている。この場合、トランスポンダ18は、図7に示すように、RFパワーを受信することで作動すると、自動的に、上記データフォーマットで、システム識別IDデータ、マスターキーグループIDデータおよび鍵IDデータを送信するようになっている。なお、システム識別IDデータ、マスターキーグループIDデータおよび鍵IDデータの目的およびその内容は、前述した通りである。

#### 【0031】A-4. 自動記録管理装置

次に、図8は、上述したリーダ1で記録した錠の開閉記録(入退室記録)を集計する自動記録管理装置の構成を示す概念図である。図において、無線部14は、前述したように、リーダ1において、システム運用データとして記録した、解錠・施錠された日時、解錠・施錠に用いられたトランスポンダ(鍵またはカード)を識別するための鍵IDデータ(個別かマスタか)を送信する。無線部14から送信されたシステム運用データは、所定の場所に設置された自動記録管理装置の無線部27により受信される。

【0032】自動記録管理部20は、所定の管理プログラムが実行される端末(パーソナルコンピュータ、ワークステーション等)30、上記無線部31、およびプリンタ32から構成されている。端末30は、所定の管理プログラムを実行し、複数のリーダから無線部14から送信されてくるシステム運用データを、無線部31により受信し、図示しない大容量記憶装置(ハードディスク等)に記憶し、所定のフォーマットでプリンタ32で印字出力する。なお、必要に応じて、集計する場合には、例えばRS-232C等のインターフェースを介して、ノートパソコン等をリーダ1に接続し、リーダ1に記録した上記情報を管理するようにしてもよい。

#### 【0033】B. 実施例の動作

次に、上述した実施例による保管庫に設けられたリーダ1および鍵に内蔵されたトランスポンダ18の動作について説明する。なお、以下では、上述したリーダ、トランスポンダ、データフォーマットの組み合わせに応じて、以下のケースについて各々の動作を説明する。

- ①CPU有り、ID更新機能有り
- ②CPU有り、ID更新機能無し
- ③CPU無し、ID更新機能有り
- ④CPU無し、ID更新機能無し

また、以下では、CPU有り、ID更新機能有り・無し、およびCPU無し、ID更新機能有り・無しにおけるIDデータ設定処理の動作についても説明する。

【0034】B-1. 解錠・施錠処理 (①CPU有り、ID更新機能有り)

まず、CPU23を備えるトランスポンダ (ID更新機能有り) 18を用いた場合における解錠処理について説明する。ここで、図9および図10は、CPU23を備えるトランスポンダ (ID更新機能有り) 18における、リーダ1およびトランスポンダ18での解錠処理の動作を説明するためのフローチャートである。

【0035】まず、保管庫のリーダ1では、通常、図9に示すステップS12、S14、S16、S32、S30からなるループで、RFパワー信号を所定時間間隔で送信する。これに対して、作業者が保管庫の鍵穴21に鍵を挿入すると、鍵に内蔵されたトランスポンダ18は、上記RFパワー信号を受信することで作動し、図10に示すステップS40で、EEPROM24からシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを読み込む。次に、ステップS42で、図4に示すデータフォーマットで、システム識別IDデータを送信する。

【0036】リーダ1では、ステップS14で、上記システム識別IDデータを受信し、ステップS16で、自身のEEPROM9に予め設定されているシステム識別IDデータと照合し、一致すれば、ステップS18に進み、マスタ・キー・グループIDデータ要求コマンドを送信する。これに対して、鍵のトランスポンダ18では、ステップS44で、上記マスタ・キー・グループIDデータ要求コマンドを受信すると、ステップS46で、ステップS40で読み出したマスタ・キー・グループIDデータを図4に示すデータフォーマットで送信する。リーダ1では、ステップS20で、上記マスタ・キー・グループIDデータを受信する。保管庫のリーダ1では、上記ステップS18、S20、鍵のトランスポンダ18では、上記ステップS44、S46を繰り返すことにより、鍵IDデータ要求コマンドの送受信、および鍵IDデータの送受信を行い、図4に示すデータフォーマットで鍵IDデータを授受する。

【0037】次に、保管庫のリーダ1では、ステップS22で、上記マスタ・キー・グループIDデータおよび鍵IDデータを、EEPROM9に予め設定されているIDデータと照合することにより、一致するか否かを判断し、それぞれ一致すると、ステップS26で、新たなIDデータ (マスタ・キー・グループIDデータまたは/および鍵IDデータ) を乱数によって生成し、EEPROM9のIDデータを更新し、記憶する。次に、ステップS28で、上記新たなIDデータ (マスタ・キー・グループIDデータまたは/および鍵IDデータ) を送信する。

【0038】これに対して、鍵のトランスポンダ18では、ステップS48で、上記新たなIDデータ (マスタ・キー・グループIDデータまたは/および鍵IDデータ)

タ)を受信し、該新たなIDデータで、EEPROM24のIDデータを書き換え、更新する。

【0039】さらに、保管庫のリーダ1では、ステップS30で、システム運用データとして、解錠した日時、解錠に用いられたトランスポンダ (鍵またはカード) を識別するための鍵IDデータ (個別かマスタか) を記録する。リーダ1は、上記システム運用データを、無線部14により定期的に送信する。該システム運用データは、自動記録管理装置20の無線部31により受信され、端末30により集計され、所定のフォーマットでプリンタ32で印字出力される。

【0040】また、リーダ1において、ステップS16で、何らのデータを受信しない場合、トランスポンダ18から送信されたシステム識別IDが自身のものと一致しない場合、あるいは、ステップS22で、トランスポンダ18から送信されたマスタ・キー・グループIDデータあるいは鍵IDデータが自身のものと一致しない場合には、ステップS32で、防犯および警報システムを作動させた後、上述したステップS30で、システム運用データを記録し、ステップS12に戻る。以下、ステップS12以降を繰り返し実行する。

【0041】B-2. 解錠・施錠処理 (②CPU有り、ID更新機能無し)

次に、CPU23を備えるトランスポンダ (ID更新機能無し) 18を用いた場合における解錠処理について説明する。ここで、図11および図12は、CPU23を備えるトランスポンダ (ID更新機能無し) 18における、リーダ1およびトランスポンダ18での解錠処理の動作を説明するためのフローチャートである。

【0042】まず、リーダ1では、通常、図11に示すステップS62、S64、S66、S78、S76からなるループで、RFパワー信号を所定時間間隔で送信する。これに対して、作業者が保管庫の鍵穴21に鍵を挿入すると、鍵に内蔵されたトランスポンダ18は、上記RFパワー信号を受信することで作動し、図12に示すステップS80で、EEPROM24からシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを読み込む。次に、ステップS82で、図4に示すデータフォーマットでシステム識別IDデータを送信する。

【0043】リーダ1では、ステップS64で、上記システム識別IDデータを受信し、ステップS66で、自身のEEPROM9に予め設定されているシステム識別IDデータと照合し、一致すれば、ステップS68に進み、マスタ・キー・グループIDデータ要求コマンドを送信する。

【0044】これに対して、鍵のトランスポンダ18では、ステップS84で、上記マスタ・キー・グループIDデータ要求コマンドを受信すると、ステップS86で、ステップS80で読み出したマスタ・キー・グループ



ブIDデータを図4に示すデータフォーマットで送信する。リーダ1では、ステップS70で、上記マスタ・キー・グループIDデータを受信する。そして、保管庫のリーダ1では、上記ステップS68、S70、鍵のトランスポンダ18では、上記ステップS84、S86を繰り返すことにより、鍵IDデータ要求コマンドの送受信、および鍵IDデータの送受信を行い、図4に示すデータフォーマットで鍵IDデータを授受する。

【0045】次に、保管庫のリーダ1では、ステップS72で、上記マスタ・キー・グループIDデータおよび鍵IDデータを、EEPROM9に予め設定されているデータと照合することにより、一致するか否かを判断し、それぞれ一致すると、ステップS76で、システム運用データとして、解錠した日時、解錠に用いられたトランスポンダ18を識別するための鍵IDデータ（個別かマスタか）を記録する。リーダ1は、上記システム運用データを、無線部14により定期的に送信する。該システム運用データは、自動記録管理装置20の無線部31により受信され、端末30により集計され、所定のフォーマットでプリンタ32で印字出力される。

【0046】また、リーダ1において、ステップS66で、何らのデータを受信しない場合、トランスポンダ18から送信されたシステム識別IDが自身のものと一致しない場合、あるいは、ステップS72で、トランスポンダ18から送信されたマスタ・キー・グループIDデータあるいは鍵IDデータが自身のものと一致しない場合には、ステップS78で、防犯および警報システムを作動させた後、上述したステップS76で、システム運用データを記録し、ステップS62に戻る。以下、ステップS62以降を繰り返し実行する。

【0047】B-3. 解錠・施錠処理（③CPU無し、ID更新機能有り）

次に、CPUを備えていないトランスポンダ（ID更新機能有り）18を用いた場合における解錠処理について説明する。ここで、図13および図14は、CPUを備えていないトランスポンダ（ID更新機能有り）18における、リーダ1およびトランスポンダ18での解錠処理の動作を説明するためのフローチャートである。

【0048】まず、保管庫のリーダ1では、通常、図13に示すステップS92、S94、S96、S106、S104からなるループで、RFパワー信号を所定時間間隔で送信する。これに対して、作業者が保管庫の鍵穴21に鍵を挿入すると、鍵に内蔵されたトランスポンダ18は、上記RFパワー信号を受信することで作動し、図14に示すステップS110で、EEPROM27からシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを読み込む。次に、ステップS112で、図6に示すデータフォーマットで、システム識別IDデータマスタ・キー・グループIDデータおよび鍵IDデータを送信する。

【0049】リーダ1では、ステップS94で、上記システム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを受信し、ステップS96で、自身のEEPROM9に予め設定されているシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータと照合し、一致すれば、ステップS100で、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を乱数によって生成し、EEPROM9のIDデータを更新し、記憶する。次に、ステップS102で、上記新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を送信する。

【0050】これに対して、鍵のトランスポンダ18では、ステップS114で、上記新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を受信し、ステップS116で、該新たなIDデータで、EEPROM27のIDデータを書き換え、更新する。

【0051】さらに、保管庫のリーダ1では、ステップS104で、システム運用データとして、解錠した日時、解錠に用いられたトランスポンダ18を識別するための鍵IDデータ（個別かマスタか）を記録する。リーダ1は、上記システム運用データを、無線部14により定期的に送信する。該システム運用データは、自動記録管理装置20の無線部31により受信され、端末30により集計され、所定のフォーマットでプリンタ32で印字出力される。

【0052】また、リーダ1において、ステップS96で、何らのデータを受信しない場合、トランスポンダ18から送信されたシステム識別ID、マスタ・キー・グループIDデータまたは鍵IDデータのいずれか1つでも自身のものと一致しない場合には、ステップS106で、防犯および警報システムを作動させた後、上述したステップS104で、システム運用データを記録し、ステップS92に戻る。以下、ステップS92以降を繰り返し実行する。

【0053】B-4. 解錠・施錠処理（④CPU無し、ID更新機能無し）

次に、CPUを備えていないトランスポンダ（ID更新機能無し）18を用いた場合における解錠処理について説明する。ここで、図15および図16は、CPUを備えていないトランスポンダ（ID更新機能無し）18における、リーダ1およびトランスポンダ18での解錠処理の動作を説明するためのフローチャートである。

【0054】まず、保管庫のリーダ1では、通常、図15に示すステップS122、S124、S126、S132、S130からなるループで、RFパワー信号を所定時間間隔で送信する。これに対して、作業者が保管庫の鍵穴21に鍵を挿入すると、鍵に内蔵されたトランスポンダ18は、上記RFパワー信号を受信することで作



動し、図16に示すステップS140で、EEPROM 27からシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを読み込む。次に、ステップS142で、図6に示すデータフォーマットでシステム識別IDデータマスタ・キー・グループIDデータおよび鍵IDデータを送信する。

【0055】リーダ1では、ステップS124で、上記システム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータを受信し、ステップS126で、自身のEEPROM9に予め設定されているシステム識別IDデータ、マスタ・キー・グループIDデータおよび鍵IDデータと照合し、一致すれば、ステップS130で、システム運用データとして、解錠した日時、解錠に用いられたトランスポンダ（鍵またはカード）18を識別するための鍵IDデータ（個別かマスタか）を記録する。リーダ1は、上記システム運用データを、無線部25により定期的に送信する。該システム運用データは、自動記録管理装置20の無線部31により受信され、端末30により集計され、所定のフォーマットでプリンタ32で印字出力される。

【0056】また、リーダ1において、ステップS126で、トランスポンダ18から送信されたシステム識別ID、マスタ・キー・グループIDデータまたは鍵IDデータのいずれか1つでも自身のものと一致しない場合には、ステップS132で、防犯および警報システムを作動させた後、上述したステップS130で、システム運用データを記録し、ステップS122に戻る。以下、ステップS122以降を繰り返し実行する。

【0057】このように、解錠・施錠処理においては、作業者が保管庫の鍵穴21に鍵を挿入すると、鍵に内蔵されたトランスポンダ18は、リーダ1からのRFパワーを受信することで、自動的に、IDデータを送信することになる。そして、IDデータが一致すれば、そのときの日時や、トランスポンダ18のIDデータが記録される。そして、該記録された情報は、所定のタイミングで自動記録管理装置20の無線部31により受信され、端末30により集計され、所定のフォーマットでプリンタ32で印字出力される。したがって、保管庫の解錠・施錠の日時、そのときに使用されたトランスポンダ18を自動的に管理することができる。また、保管庫ではなく、部屋とすれば、入退室を自動的に管理することができる。

【0058】B-5. IDデータ設定処理（CPU有り）

次に、CPU23を備えるトランスポンダ18を用いた場合におけるIDデータ設定処理について説明する。当該IDデータ設定処理は、リーダ1およびトランスポンダ18の出荷時、鍵の紛失などの場合に、リーダ1およびトランスポンダ18に既に設定されているIDデータ（マスターキーグループIDデータまたは／および鍵ID

Dデータ）を変更する場合に実行される。ここで、図17ないし図19は、CPU23を備えるトランスポンダ（ID更新機能有り・無し）18における、設定器（図示略）、リーダ1およびトランスポンダ18におけるIDデータ設定処理の動作を説明するためのフローチャートである。

【0059】図示しない設定器では、まず、ステップS150で、新IDデータ（マスターキーグループIDデータまたは／および鍵IDデータ）が設定され、リーダ1のデータ通信範囲内に移動させられる。そして、リーダ1のデータ通信範囲内に移動すると、ステップS152で、保管庫のリーダ1に対してシステム識別IDデータを送信する。

【0060】これに対して、保管庫のリーダ1では、設定器が該リーダの通信範囲内に移動した時点で、図18に示すステップS160において、設定器から送信されるデータ（システム識別ID）を自動的に受信する。次に、データを受信すると、ステップS162で、受信したデータがEEPROM9に予め設定されているシステム識別IDと一致するか照合し、一致すると、ステップS164に進み、設定器に対してマスタ・キー・グループIDデータ要求コマンドを送信する。

【0061】設定器では、ステップS154で、リーダ1からマスタ・キー・グループIDデータ要求コマンドを受信すると、ステップS156で、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を設定するというコマンド、言い換えると、マスタ・キー・グループIDデータ要求コマンドに対するマスタ・キー・グループIDデータ以外の所定のデータを、保管庫のリーダ1に対して送信した後、ステップS158で、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）をリーダ1に対して送信する。

【0062】保管庫のリーダ1では、ステップS166で、マスタ・キー・グループIDデータ要求に対するデータを受信し、ステップS168で、受信したデータが新たなIDデータの設定データ（コマンド）であるか判断し、設定データであると、ステップS170に進み、設定器から送信された新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を受信する。次に、ステップS172で、受信した新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）でEEPROM9に格納されているIDデータを更新し、記憶する。そして、ステップS174で、鍵のトランスポンダ18に対して、上記新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を送信する。

【0063】これに対して、鍵のトランスポンダ18では、当該トランスポンダ18がリーダのデータ通信範囲にあると、図19に示すステップS190で、新IDデ

ータを自動的に受信し、ステップS192で、受信した新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）でEEPROM24に格納されているIDデータを更新し、記憶する。

【0064】一方、リーダ1では、図18に示すステップS176で、システムのIDデータ変更完了処理として、鍵のトランスポンダ18との間でIDデータを授受することにより、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）の変更を確認する。そして、ステップS178で、システム運用データとして、IDデータを変更（設定）した日時、トランスポンダ（鍵）18を識別するための鍵IDデータ（個別かマスタか）、およびIDデータを変更（設定）したことを記録する。リーダ1は、上記システム運用データを、無線部14により定期的に送信する。該システム運用データは、自動記録管理装置20の無線部31により受信され、端末30により集計され、所定のフォーマットでプリンタ32で印字出力される。

【0065】また、保管庫のリーダ1において、ステップS162で、設定器から送信されたシステム識別IDと自身のシステム識別IDとが一致しない場合、あるいは、ステップS168で、受信したデータが新たなIDデータの設定データ（コマンド）でない場合には、ステップS180で、防犯および警報システムを作動させる。

【0066】このように、上述した処理によれば、CPU23を備えているトランスポンダ18を用いる場合には、新たなIDデータを設定する際に、システムIDデータを保管庫のリーダ1に送信するとともに、リーダ1からのマスタ・キー・グループIDデータ要求コマンドに対して所定のデータを送信することで、該リーダ1を自動的に新たなIDデータ受信処理へ移行させることができる。したがって、リーダ1およびトランスポンダ18は、通常の前データ授受処理と同様のデータ授受処理を行うことで、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を設定することができる。

【0067】B-6. IDデータ設定処理（CPU無し）

次に、CPUを備えていないトランスポンダ18を用いた場合におけるIDデータ設定処理について説明する。ここで、図20ないし図22は、CPUを備えていないトランスポンダ（ID更新機能有り・無し）18における、設定器（図示略）、リーダ1およびトランスポンダ18におけるIDデータ設定処理の動作を説明するためのフローチャートである。

【0068】図示しない設定器では、まず、図20に示すステップS200で、新IDデータ（マスターキーグループIDデータまたは／および鍵IDデータ）が設定され、リーダ1のデータ通信範囲内に移動させられる。

そして、リーダ1のデータ通信範囲内に移動すると、ステップS202で、保管庫のリーダ1に対して、設定器を識別するための設定器IDデータを送信した後、ステップS204で、新たなIDデータを送信する。

【0069】これに対して、保管庫のリーダ1では、設定器が通信範囲内に移動した時点で、図21に示すステップS210において、設定器から送信される設定器IDデータを自動的に受信する。次に、設定器IDデータを受信すると、ステップS212で、受信した設定器IDデータが所定のデータであるか照合し、所定のデータである場合には、ステップS214に進み、設定器から送信される新たなIDデータを受信する。

【0070】次に、リーダ1は、ステップS216で、受信した新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）でEEPROM9に格納されているIDデータを更新し、記憶する。そして、ステップS218で、鍵のトランスポンダ18に対して、上記新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）を送信する。

【0071】これに対して、鍵のトランスポンダ18では、当該トランスポンダ18がリーダ1のデータ通信範囲にあると、図22に示すステップS230で、新IDデータを自動的に受信し、ステップS232で、受信した新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）でEEPROM27に格納されているIDデータを更新し、記憶する。

【0072】一方、リーダ1では、図21に示すステップS220で、システムのIDデータ変更完了処理として、鍵のトランスポンダ18との間でIDデータを授受することにより、新たなIDデータ（マスタ・キー・グループIDデータまたは／および鍵IDデータ）の変更を確認する。そして、ステップS222で、システム運用データとして、IDデータを変更（設定）した日時、トランスポンダ（鍵）18を識別するための鍵IDデータ（個別かマスタか）およびIDデータを変更（設定）したことを記録する。リーダ1は、上記システム運用データを、無線部14により定期的に送信する。該システム運用データは、自動記録管理装置20の無線部31により受信され、端末30により集計され、所定のフォーマットでプリンタ32で印字出力される。

【0073】また、保管庫のリーダ1において、ステップS212で、設定器から送信された設定器IDデータが所定のデータでない場合には、ステップS224で、防犯および警報システムを作動させる。

【0074】このように、上述した処理によれば、CPU23を備えていないトランスポンダ18を用いる場合、新たなIDデータを設定する際に、設定器固有の設定器IDデータを保管庫のリーダ1に送信することで、該リーダ1を自動的に新たなIDデータ受信処理へ移行

させることができる。したがって、リーダ 1 およびトランスポンダ 1 8 は、通常のデータ授受処理と同様のデータ授受処理を行うことで、新たな ID データ（マスタ・キー・グループ ID データまたは／および鍵 ID データ）を設定することができる。

【0075】なお、上記実施例では、トランスポンダ 1 8 を内蔵した 1 つの鍵で、錠を解錠する保管庫について説明したが、より安全性を高めるために、複数の鍵が揃った時点で錠を解錠するような保管庫であってもよい。この場合、各鍵のトランスポンダ 1 8 には、異なる ID データを記憶させており、リーダ 1 側では、上記複数の ID データの全てが一致しなければ、警報を発するようにすればよい。また、鍵のトランスポンダ 1 8 と保管庫のリーダ 1 との ID データが不一致である場合、防犯および警報システムを作動させるようにしたが、具体的には、警報音を鳴らしたり、防犯カメラを作動させたり、通信回線を介して通報したりというように、少なくとも 1 つ、あるいはこれらを組み合わせて用いるようにしてもよい。さらに、上記実施例では、リーダ 1 と自動記録管理装置 2 0 との間で、無線により情報を授受するようにしたが、これに限らず、有線あるいは電話回線を介して送信するようにしてもよい。

【0076】また、上記実施例では、トランスポンダ 1 8 を内蔵しない鍵の使用を考慮していないが、図 1 に示すように、P I O 1 2 を介して、保管庫の扉の開閉を検知するマイクロスイッチ 3 3 を設けることにより、トランスポンダ 1 8 を内蔵しない鍵によって解錠／施錠され、扉が開閉された場合、上記マイクロスイッチ 3 3 により扉の開閉を検知し、そのときの日時等を記憶するようにしてもよい。これにより、トランスポンダ 1 8 を内蔵していない鍵を使用した場合であっても、入退室やメンテナンス等を容易に管理することができる。さらに、トランスポンダ 1 8 を内蔵しない鍵が使用された場合には、不正使用であると判断し、防犯および警報システムを作動させるとともに、上記日時等の記録を行うようにしてもよい。

#### 【0077】

【発明の効果】請求項 1 記載の発明によれば、応答装置が保管庫に近接すると、読み取り装置の高周波発生手段からの高周波磁界を電力とし、第 1 の送信手段から第 1 の記憶手段に記憶されている応答装置識別データが送信され、該応答装置識別データが読み取り装置の第 2 の記憶手段に記憶されている応答装置識別データとが一致すると、記録手段に計時手段による現在時刻を記録するようにしたので、入退室やメンテナンス時に生じる、錠の開閉を把握することにより、入退室やメンテナンス等を容易に管理することができるという利点が得られる。

【0078】また、請求項 2 記載の発明によれば、前記第 1 受信手段によって受信された応答装置識別データと前記第 2 の記憶手段に記憶されている応答装置識別デー

タとが一致しない場合、警告手段によって警告を発するようにしたので、より機密性を向上させることができ、より安全性を向上させることができるという利点が得られる。

【0079】また、請求項 3 記載の発明によれば、前記高周波発生手段によって、所定時間間隔で、高周波磁界を発生するようにしたので、電力消費を低減することができるという利点が得られる。

【0080】また、請求項 4 記載の発明によれば、前記応答装置および前記読み取り装置は、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび保管庫の設置地域を識別するマスタ・キー・グループ識別データを授受するようにしたので、入退室やメンテナンス時に生じる、錠の開閉を把握することにより、入退室やメンテナンス等を容易に、かつより厳密に管理することができるという利点が得られる。

【0081】また、請求項 5 記載の発明によれば、前記応答装置に、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第 2 の制御手段を備え、前記応答装置および前記読み取り装置との間で、前記所定の通信プロトコルに従って、前記システム識別データ、前記マスタ・キー・グループ識別データおよび前記応答装置識別データを授受するようにしたので、入退室やメンテナンス時に生じる、錠の開閉を把握することにより、入退室やメンテナンス等を容易に、かつより厳密に管理することができるという利点が得られる。

【0082】また、請求項 6 記載の発明によれば、電気錠を解錠する度に、認証に必要な応答装置識別データを書き換えるようにしたので、より機密性を向上させることができ、より安全性を向上させることができるとともに、応答装置の不正なコピーを防止できるという利点が得られる。

【0083】また、請求項 7 記載の発明によれば、前記応答装置識別データおよびマスタ・キー・グループ識別データを外部設定装置により無線通信により書換可能とするようにしたので、応答装置（鍵）の紛失、盗難が生じた場合でも、非接触で識別データの書き換えができるので、ハードウェアを取り替えることなく、更新できるという利点が得られる。

【0084】また、請求項 8 ないし 1 1 記載の発明によれば、読み取り手段の記録手段に記憶された情報を出力手段により、無線、有線または電話回線を介して外部機器に送出し、外部機器として設けた管理手段において、前記出力手段から出力される情報を受信手段により受信し、該受信した情報を集計手段により集計するようにしたので、入退室やメンテナンス時に生じる、錠の開閉を把握することにより、入退室やメンテナンス等を容易に、かつより厳密に管理することができるという利点が得られる。

【0085】また、請求項12記載の発明によれば、検出手段により、扉の開閉を検知するようにしたので、応答装置を内蔵しない鍵によって解錠／施錠され、扉が開閉された場合、上記検出手段により扉の開閉を検知し、そのときの日時等を記憶するようにしてもよい。これにより、応答装置を内蔵していない鍵を使用した場合であっても、入退室やメンテナンス等を容易に管理することができるという利点が得られる。

【図面の簡単な説明】

【図1】本発明の実施例による鍵開閉管理システムの構成を示すブロック図である。

【図2】トランスポンダが内蔵された鍵（カード形状）とリーダが内蔵された保管庫の外観構成を示す斜視図である。

【図3】トランスポンダのより詳細な構成例を示すブロック図である。

【図4】トランスポンダがCPUを備える場合におけるリーダとトランスポンダとで授受されるデータフォーマットを示す概念図である。

【図5】トランスポンダがCPUを備える場合におけるリーダとトランスポンダとの間でのデータ授受を示す概念図である。

【図6】トランスポンダがCPUを備えない場合におけるリーダとトランスポンダとで授受されるデータフォーマットを示す概念図である。

【図7】トランスポンダがCPUを備えない場合におけるリーダとトランスポンダとの間でのデータ授受を示す概念図である。

【図8】CPUを備えるトランスポンダ（ID更新機能有り）の場合におけるリーダでの解錠処理の動作を説明するためのフローチャートである。

【図9】CPUを備えるトランスポンダ（ID更新機能有り）の場合におけるトランスポンダでの解錠処理の動作を説明するためのフローチャートである。

【図10】CPUを備えるトランスポンダ（ID更新機能無し）の場合におけるリーダでの解錠処理の動作を説明するためのフローチャートである。

【図11】CPUを備えるトランスポンダ（ID更新機能無し）の場合におけるトランスポンダでの解錠処理の動作を説明するためのフローチャートである。

【図12】CPUを備えていないトランスポンダ（ID更新機能有り）の場合におけるリーダでの解錠処理の動作を説明するためのフローチャートである。

【図13】CPUを備えていないトランスポンダ（ID更新機能有り）の場合におけるトランスポンダでの解錠処理の動作を説明するためのフローチャートである。

【図14】CPUを備えていないトランスポンダ（ID更新機能無し）の場合におけるリーダでの解錠処理の動作を説明するためのフローチャートである。

【図15】CPUを備えていないトランスポンダ（ID

更新機能無し）の場合におけるトランスポンダでの解錠処理の動作を説明するためのフローチャートである。

【図16】CPUを備えるトランスポンダ（ID更新機能有り・無し）の場合における設定器（図示略）でのIDデータ設定処理の動作を説明するためのフローチャートである。

【図17】CPUを備えるトランスポンダ（ID更新機能有り・無し）の場合におけるリーダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図18】CPUを備えるトランスポンダ（ID更新機能有り・無し）の場合におけるトランスポンダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図19】CPUを備えていないトランスポンダ（ID更新機能有り・無し）の場合における設定器（図示略）でのIDデータ設定処理の動作を説明するためのフローチャートである。

【図20】CPUを備えていないトランスポンダ（ID更新機能有り・無し）の場合におけるリーダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図21】CPUを備えていないトランスポンダ（ID更新機能有り・無し）の場合におけるトランスポンダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【符号の説明】

- 1 リーダ
- 2 変調回路（高周波発生手段、第2の送信手段）
- 3 RFパワー送信機（高周波発生手段、第2の送信手段）
- 4 DATA受信回路（第1の受信手段）
- 5 DATA復調回路（第1の受信手段）
- 6 MPU
- 7 SIO
- 8 CPU（第1の制御手段、応答装置識別データ生成手段、第1の更新手段、計時手段）
- 9 EEPROM（第2の記憶手段）
- 10 ROM
- 11 RAM
- 12 PIO
- 13 NG表示用LED（警告手段）
- 14 無線部（出力手段）
- 15 スイッチングレギュレータ
- 16, 17 アンテナ
- 18 トランスポンダ
- 19 アンテナ
- 20 自動記録管理装置
- 22 送受信回路（第1の送信手段、第2の受信手段、第2の更新手段）
- 23 CPU（第2の制御手段）

24 EEPROM (第1の記憶手段)

26 送受信回路 (第1の送信手段、第2の受信手段、第2の更新手段)

27 EEPROM (第1の記憶手段)

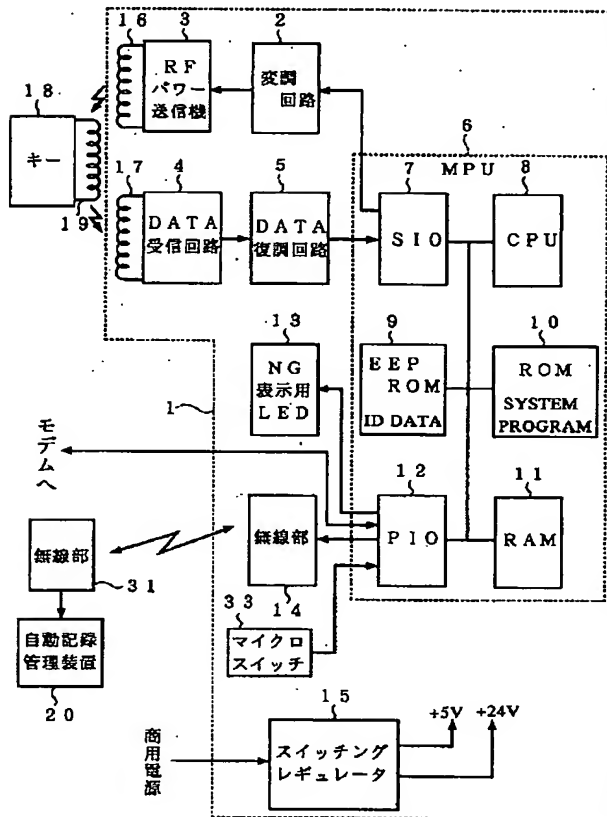
30 端末 (管理手段)

31 無線部 (受信手段)

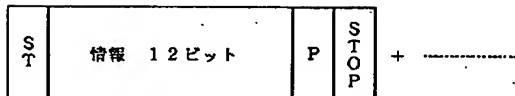
32 プリンタ

33 マイクロスイッチ (検出手段)

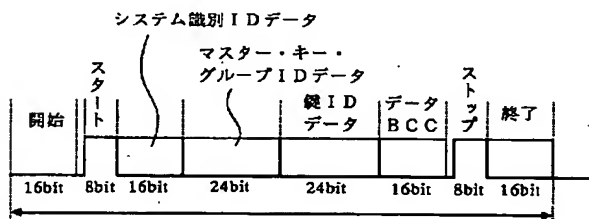
【図1】



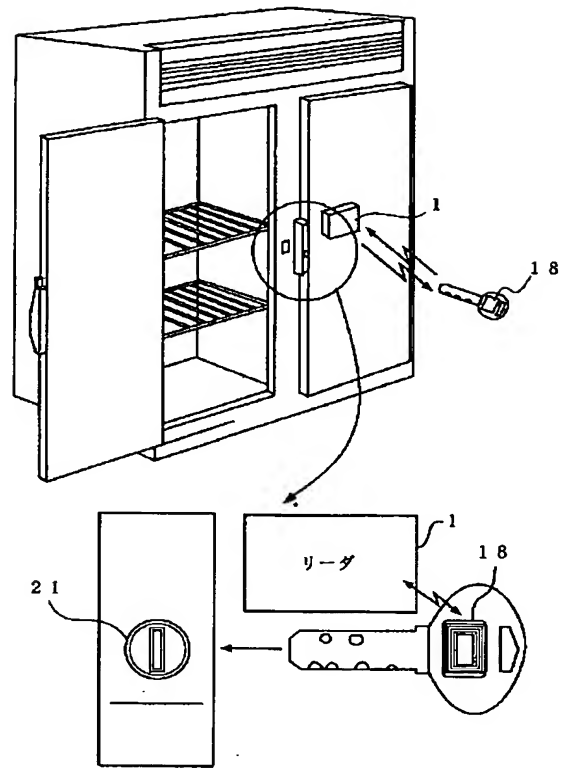
【図4】



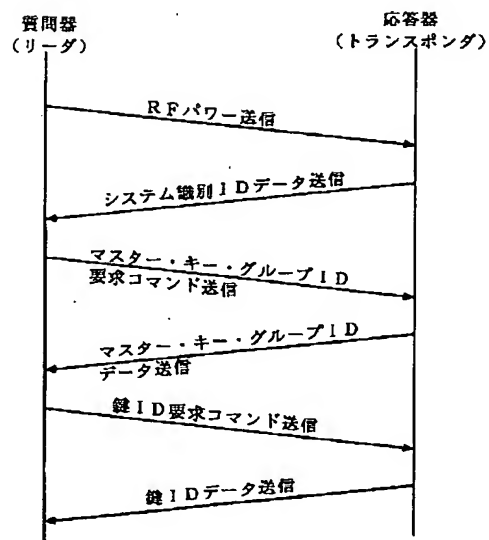
【図6】



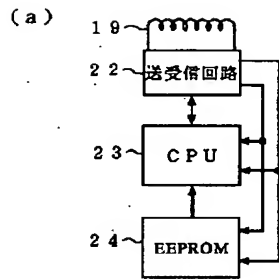
【図2】



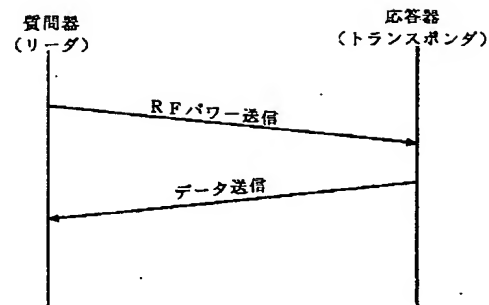
【図5】



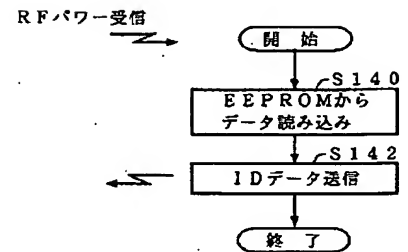
【図3】



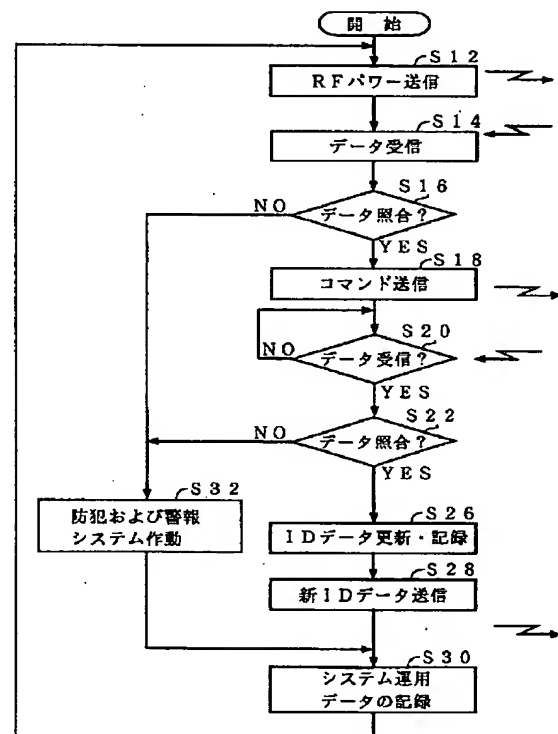
【図7】



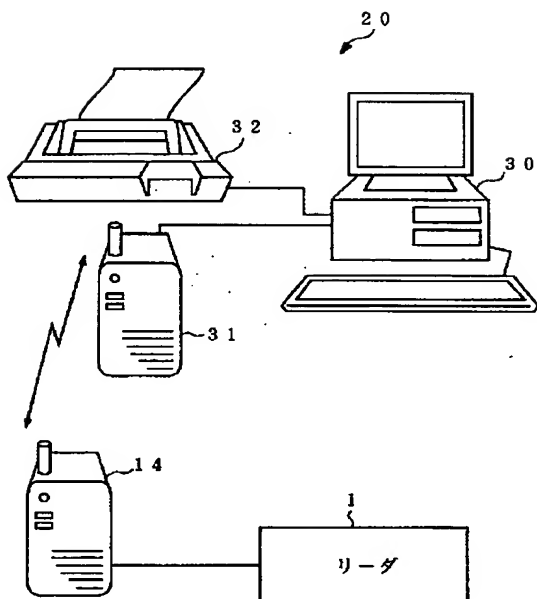
【図16】



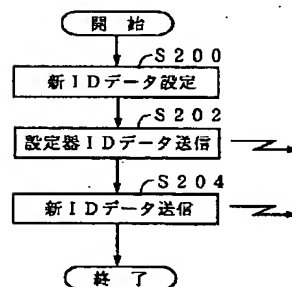
【図9】



【図8】

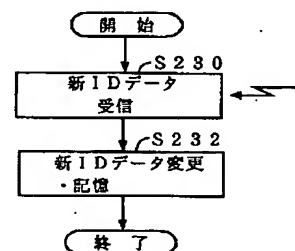


【図20】

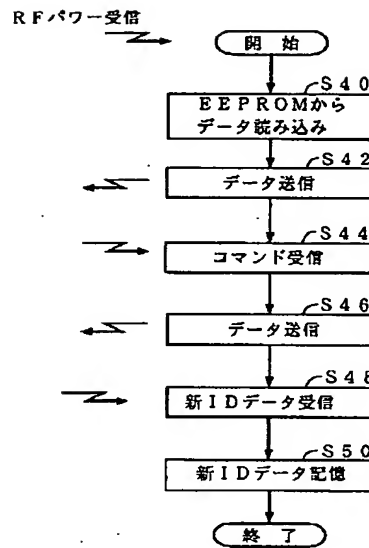


【図22】

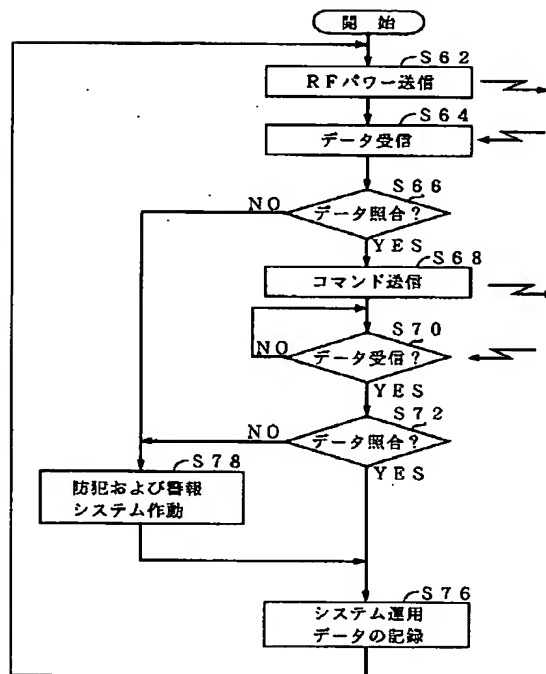
IDデータ設定時のトランスポンダ



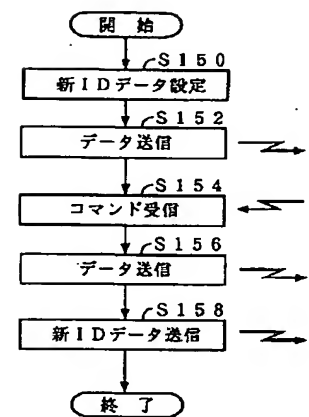
【図10】



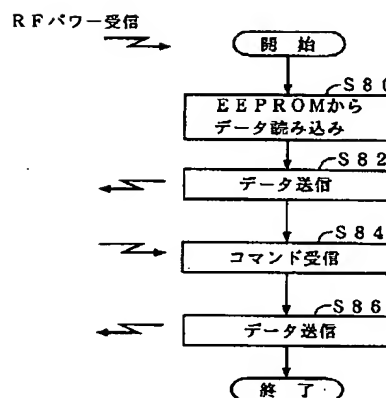
【図11】



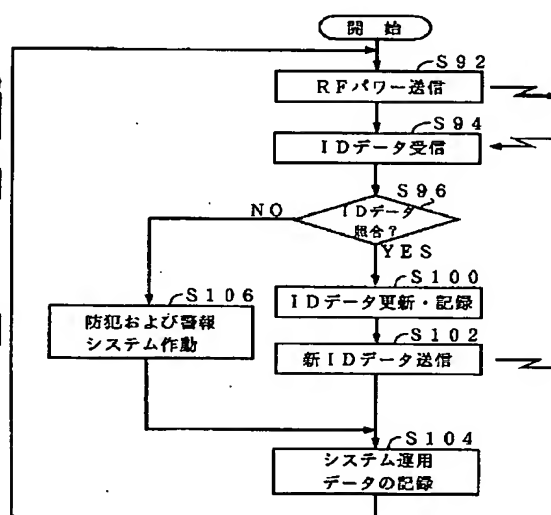
【図17】



【図12】

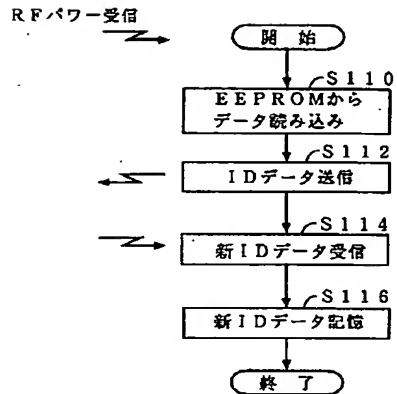


【図13】

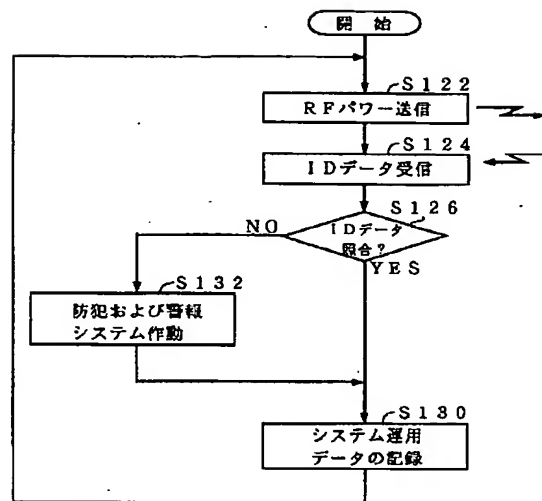




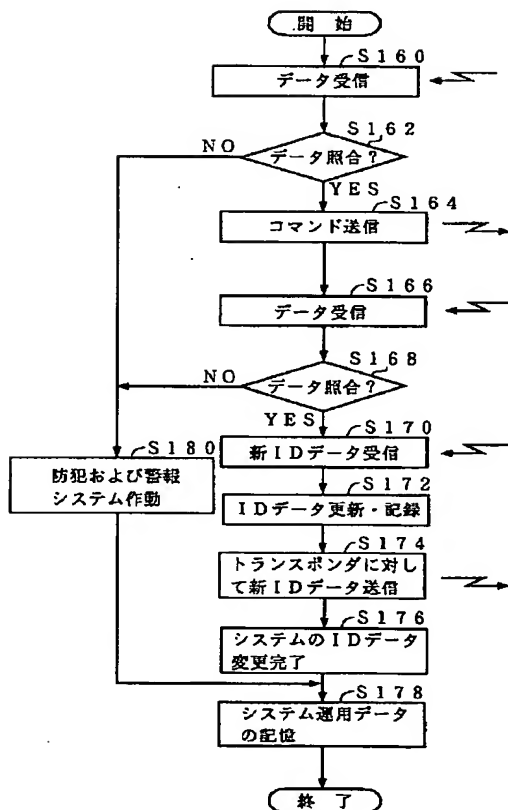
【図14】



【図15】

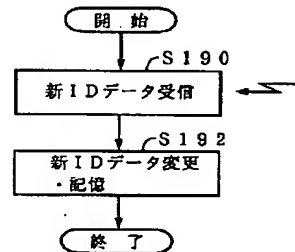


【図18】

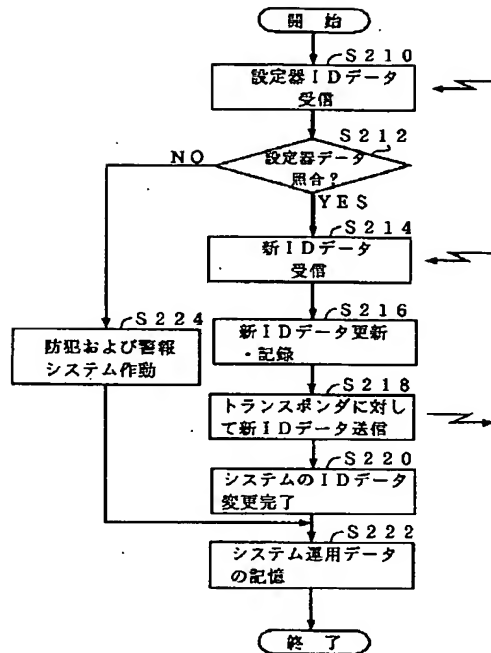


【図19】

IDデータ設定時のトランスポンダ



【図21】



## 【手続補正書】

【提出日】平成9年2月5日

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】図面の簡単な説明

【補正方法】変更

【補正内容】

【図面の簡単な説明】

【図1】本発明の実施例による鍵開閉管理システムの構成を示すブロック図である。

【図2】トランスポンダが内蔵された鍵（カード形状）とリーダが内蔵された保管庫の外観構成を示す斜視図である。

【図3】トランスポンダのより詳細な構成例を示すブロック図である。

【図4】トランスポンダがCPUを備える場合におけるリーダとトランスポンダとで授受されるデータフォーマットを示す概念図である。

【図5】トランスポンダがCPUを備える場合におけるリーダとトランスポンダとの間でのデータ授受を示す概念図である。

【図6】トランスポンダがCPUを備えない場合におけるリーダとトランスポンダとで授受されるデータフォーマットを示す概念図である。

【図7】トランスポンダがCPUを備えない場合にお

けるリーダとトランスポンダとの間でのデータ授受を示す概念図である。

【図8】CPUを備えるトランスポンダ（ID更新機能有り）の場合におけるリーダでの解錠処理の動作を説明するためのフローチャートである。

【図9】CPUを備えるトランスポンダ（ID更新機能有り）の場合におけるトランスポンダでの解錠処理の動作を説明するためのフローチャートである。

【図10】CPUを備えるトランスポンダ（ID更新機能無し）の場合におけるリーダでの解錠処理の動作を説明するためのフローチャートである。

【図11】CPUを備えるトランスポンダ（ID更新機能無し）の場合におけるトランスポンダでの解錠処理の動作を説明するためのフローチャートである。

【図12】CPUを備えていないトランスポンダ（ID更新機能有り）の場合におけるリーダでの解錠処理の動作を説明するためのフローチャートである。

【図13】CPUを備えていないトランスポンダ（ID更新機能有り）の場合におけるトランスポンダでの解錠処理の動作を説明するためのフローチャートである。

【図14】CPUを備えていないトランスポンダ（ID更新機能無し）の場合におけるリーダでの解錠処理の動作を説明するためのフローチャートである。

【図15】CPUを備えていないトランスポンダ（ID

更新機能無し)の場合におけるトランスポンダでの解錠処理の動作を説明するためのフローチャートである。

【図16】CPUを備えるトランスポンダ(ID更新機能有り・無し)の場合における設定器(図示略)でのIDデータ設定処理の動作を説明するためのフローチャートである。

【図17】CPUを備えるトランスポンダ(ID更新機能有り・無し)の場合におけるリーダーでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図18】CPUを備えるトランスポンダ(ID更新機能有り・無し)の場合におけるトランスポンダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図19】CPUを備えていないトランスポンダ(ID更新機能有り・無し)の場合における設定器(図示略)でのIDデータ設定処理の動作を説明するためのフローチャートである。

【図20】CPUを備えていないトランスポンダ(ID更新機能有り・無し)の場合におけるリーダーでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図21】CPUを備えていないトランスポンダ(ID更新機能有り・無し)の場合におけるトランスポンダでのIDデータ設定処理の動作を説明するためのフローチャートである。

【図22】CPUを備えていないトランスポンダ(ID更新機能有り・無し)の場合におけるIDデータ設定処理の動作を説明するためのフローチャートである。

【符号の説明】

- 1 リーダ
- 2 変調回路(高周波発生手段、第2の送信手段)

- 3 RFパワー送信機(高周波発生手段、第2の送信手段)
- 4 DATA受信回路(第1の受信手段)
- 5 DATA復調回路(第1の受信手段)
- 6 MPU
- 7 SIO
- 8 CPU(第1の制御手段、応答装置識別データ生成手段、第1の更新手段、計時手段)
- 9 EEPROM(第2の記憶手段)
- 10 ROM
- 11 RAM
- 12 PIO
- 13 NG表示用LED(警告手段)
- 14 無線部(出力手段)
- 15 スイッチングレギュレータ
- 16, 17 アンテナ
- 18 トランスポンダ
- 19 アンテナ
- 20 自動記録管理装置
- 22 送受信回路(第1の送信手段、第2の受信手段、第2の更新手段)
- 23 CPU(第2の制御手段)
- 24 EEPROM(第1の記憶手段)
- 26 送受信回路(第1の送信手段、第2の受信手段、第2の更新手段)
- 27 EEPROM(第1の記憶手段)
- 30 端末(管理手段)
- 31 無線部(受信手段)
- 32 プリンタ
- 33 マイクロスイッチ(検出手段)

## \* NOTICES \*

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

---

## CLAIMS

---

[Claim(s)]

[Claim 1] It is equipment which makes an external high-frequency field the power for driving each part. It has the 1st transmitting means which transmits the response device identification data memorized by said 1st storage means if the 1st storage means and power which memorizes the response device identification data for identifying the equipment concerned are impressed. The answerback formed in the key which an operator carries, and a RF generating means to generate said high-frequency field, The 1st receiving means which receives the response device identification data transmitted from said 1st transmitting means, The 2nd storage means which memorizes the response device identification data which specify the answerback corresponding to the equipment concerned, the time check which clocks time of day, when the response device identification data memorized by the response device identification data received by the means and said 1st receiving means and said 2nd storage means are in agreement at least -- said time check -- the lock closing motion managerial system characterized by providing the reader formed in the lock side which is equipped with a record means to record the current time by the means, and said key locks and unlocks.

[Claim 2] Said reader is a lock closing motion managerial system according to claim 1 characterized by providing the warning means which emits warning when the response device identification data memorized by the response device identification data received by said 1st receiving means and said 2nd storage means are not in agreement.

[Claim 3] Said reader is a lock closing motion managerial system according to claim 1 or 2 which is predetermined time spacing and is characterized by generating a high-frequency field with said RF generating means.

[Claim 4] Said answerback and said reader are claim 1 characterized by delivering and receiving the master key group discernment data which identify the installation area of the system discernment data and the lock which identify a system in addition to said response device identification data thru/or a lock closing motion managerial system given in three.

[Claim 5] They are claim 1 which said answerback follows a predetermined communications protocol, is equipped with the 2nd control means which controls the data transfer between said readers, and is characterized by said answerback and said reader delivering and receiving said system discernment data, said master key group discernment data, and said response device identification data according to said predetermined communications protocol thru/or a lock closing motion managerial system given in four.

[Claim 6] 2nd transmitting means by which said reader transmits data to said answerback, A response device identification data generation means to generate new response device identification data after reception of said response device identification data, It has the 1st updating means which rewrites the response device identification data memorized by said 2nd storage means by the new response device identification data generated by said response device identification data generation means. Said new response device identification data are transmitted to said answerback with said 2nd transmitting means. Said answerback The response device identification data memorized by the 2nd receiving means which receives the data which said reader transmits, and said 1st storage means Claim 1 characterized by

having the 2nd updating means rewritten by said new response device identification data received with said 2nd receiving means thru/or a lock closing motion managerial system given in five.

[Claim 7] Said response device identification data and master key group discernment data are claim 1 characterized by the ability to rewrite by radio with an external setting device thru/or a lock closing motion managerial system given in six.

[Claim 8] Said reading means is claim 1 characterized by to provide the management tool which is equipped with an output means send out the information memorized by said record means to an external instrument, and is equipped with a receiving means receive the information outputted from said output means as said external instrument, and a total means total the information received with said receiving means thru/or a lock closing-motion managerial system given in seven.

[Claim 9] Said output means is a lock closing motion managerial system according to claim 8 characterized by transmitting the information memorized by said record means by wireless.

[Claim 10] Said output means is a lock closing motion managerial system according to claim 8 characterized by transmitting the information memorized by said record means by the cable.

[Claim 11] Said output means is a lock closing motion managerial system according to claim 8 characterized by transmitting the information memorized by said record means through the telephone line.

[Claim 12] Said reader is a lock closing motion managerial system according to claim 1 characterized by providing a detection means to detect closing motion of the door opened and closed by unlocking/locking said lock.

---

[Translation done.]

## \* NOTICES \*

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the lock closing motion managerial system which performs automatically service management of close leaving management, an automatic vending machine, etc.

[0002]

[Description of the Prior Art] In close leaving management in a facility which restricts conventionally human being who does close leaving, and the time of day which carries out close leaving, when opening the lock of the door which carries out close leaving and carrying out close leaving, time of day was recorded by the time recorder etc., and it had made sign the ON appearance person, \*(ed) and gone [ who went in and out when and ]. Moreover, in the service management concerning the storage warehouse which keeps drugs, cash, goods, etc., for example, the automatic vending machine which sells goods by uninhabited, who \*\*\*\*ed for the note when it maintained (or [ having opened the lock for carrying in and taking out of an article, sales recovery exchange of goods, a supplement etc. ]), and was performing it. Moreover, even if it was which case, the above-mentioned record was periodically totaled by the manual, and synthetic management was performed.

[0003]

[Problem(s) to be Solved by the Invention] However, in a conventional close leaving managerial system and a conventional service managerial system, since the manual was performing the time of day of close leaving, register, a total, etc., there was a problem that he forgot record or a total took time amount and time and effort.

[0004] Then, this invention aims at offering the lock closing motion managerial system which can manage close leaving, a maintenance, etc. easily by grasping the closing motion of a lock produced at the time of close leaving or a maintenance.

[0005]

[Means for Solving the Problem] The lock closing motion managerial system by invention according to claim 1 for the above-mentioned purpose achievement It is equipment which makes an external high-frequency field the power for driving each part. It has the 1st transmitting means which transmits the response device identification data memorized by said 1st storage means if the 1st storage means and power which memorizes the response device identification data for identifying the equipment concerned are impressed. The answerback formed in the key which an operator carries, and a RF generating means to generate said high-frequency field, The 1st receiving means which receives the response device identification data transmitted from said 1st transmitting means, The 2nd storage means which memorizes the response device identification data which specify the answerback corresponding to the equipment concerned, the time check which clocks time of day, when the response device identification data memorized by the response device identification data received by the means and said 1st receiving means and said 2nd storage means are in agreement at least -- said time check -- it has a record means to record the current time by the means, and is characterized by providing the reader formed in the lock

side which said key locks and unlocks.

[0006] Moreover, when the response device identification data memorized by the response device identification data received by said 1st receiving means like and said 2nd storage means according to claim 2 are not in agreement, you may make it said reader possess the warning means which emits warning as a desirable mode, for example.

[0007] Moreover, said reader is good as a desirable mode as for a method according to claim 3 of being predetermined time spacing and generating a high-frequency field with said RF generating means, like, for example.

[0008] moreover -- as a desirable mode -- said answerback and said reader -- for example, -- being according to claim 4 -- like -- said response device identification data -- in addition, you may make it deliver and receive the master key group discernment data which identify the installation area of the system discernment data and the specially-equipped vehicle which identify a system

[0009] Moreover, said answerback is equipped with the 2nd control means which controls the data [ follow a predetermined communications protocol like and ] transfer according to claim 5 between said readers as a desirable mode, for example, and you may make it said answerback and said reader deliver and receive said system discernment data, said master key group discernment data, and said response device identification data according to said predetermined communications protocol.

[0010] As a desirable mode, moreover, said reader Like claim 6 publication, for example, said reader The 2nd transmitting means which transmits data to said answerback, and a response device identification data generation means to generate new response device identification data after reception of said response device identification data, It has the 1st updating means which rewrites the response device identification data memorized by said 2nd storage means by the new response device identification data generated by said response device identification data generation means. Said new response device identification data are transmitted to said answerback with said 2nd transmitting means. Said answerback You may make it have the 2nd updating means which rewrites the response device identification data memorized by the 2nd receiving means which receives the data which said reader transmits, and said 1st storage means by said new response device identification data received with said 2nd receiving means.

[0011] Moreover, it may be [ with an external setting device ] rewritable [ said response device identification data and master key group discernment data ] like for example, claim 7 publication as a desirable mode with radio.

[0012] Moreover, said reading means is equipped with an output means send out the information according to claim 8 memorized by said record means to an external instrument like, for example, and it may make possess a management tool equipped with a receiving means receive the information outputted from said output means, and a total means total the information received with said receiving means, as said external instrument as a desirable mode.

[0013] Moreover, you may make it said output means transmit the information according to claim 9 memorized by said record means by wireless like as a desirable mode, for example.

[0014] Moreover, you may make it said output means transmit the information according to claim 10 memorized by said record means by the cable like as a desirable mode, for example.

[0015] Moreover, you may make it said output means transmit the information according to claim 11 memorized by said record means through the telephone line like as a desirable mode, for example.

[0016] Moreover, you may make it said reader possess a detection means to detect closing motion of the door opened and closed by [ according to claim 12 ] unlocking/locking said lock like, for example, as a desirable mode.

[0017]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing as one example applied to lock closing motion management of a storage warehouse.

A. The block diagram 1 of the configuration A-1. reader of an example and a key (transponder) is a block diagram showing the configuration of the transponder prepared in the lock of the reader and



storage warehouse which are established in the storage warehouse by the example of this invention. Moreover, drawing 3 is the block diagram showing the more detailed example of a configuration of the above-mentioned transponder. In drawing, a reader 1 is formed in the existing storage warehouse, and consists of a modulation circuit 2, RF power transmitter 3, the DATA receiving circuit 4, the DATA demodulator circuit 5, MPU6, LED13 for NG display, relay 14, and switching regulator 15 grade. Hereafter, each part is explained.

[0018] A modulation circuit 2 carries out the FSK modulation of the predetermined signal by 125kHz, and supplies it to RF power transmitter 3. RF power transmitter 3 transmits the above-mentioned modulating signal from an antenna 16. There are RF power for operating the transponder 18 which is built in the key and which is mentioned later as the above-mentioned signal and a command for requiring various ID transmission from a transponder 18. Next, the DATA receiving circuit 4 receives the signal which is transmitted from the transponder 18 mentioned later and by which the PSK modulation was carried out by 62.5kHz with an antenna 17, and supplies it to the DATA demodulator circuit 5. The DATA demodulator circuit 5 restores to an input signal, takes out data (various kinds ID), and supplies them to SIO (serial input/output interface)7 of MPU6.

[0019] MPU6 consists of the above SIO7, CPU (central processing unit)8, EEPROM9, ROM (read-only memory)10, RAM (random access memory)11, and PIO (parallel input/output interface)12. SIO7 supplies the data from the above-mentioned DATA demodulator circuit 5 to CPU8. CPU8 executes the program stored in ROM10, and controls transmission of various commands, reception of the various data from a transponder 18, authentication of a transponder 18, record of various ID data from a transponder 18, the time check of current time, etc.

[0020] Various ID data for identifying the transponder 18 corresponding to the reader 1 concerned prepared in the storage warehouse are memorized by EEPROM9. When in other words the transponder 18 which transmits ID data which correspond with ID data memorized by this EEPROM9 approaches, Namely, if ID data memorized by ID data and EEPROM9 of a transponder 18 are in agreement when an operator fits a key over a keyhole, in order to take out the article currently kept in the storage warehouse or to carry in The time and ID data at that time are recorded.

[0021] Moreover, as mentioned above, the program performed by CPU8 is stored in ROM10. The data generated with control of the above CPU 8 are stored, or RAM11 is used as working area. Under control of CPU8, PIO12 is predetermined timing and supplies ID data of the closing motion (close leaving) time of a lock, or a transponder 18 to the wireless section 14 while it supplies the indicative data supplied from CPU8 to LED13 for NG display.

[0022] LED13 for NG display is a display turned on when inharmonious (i.e., when it is going to unlock with the key not suiting), ID data with which ID data transmitted from a transponder 18 are stored in the above EEPROM 9, and. The wireless section 14 transmits ID data of the closing motion (close leaving) time of a lock, or a transponder 18 to the automatic-recording managerial system mentioned later to predetermined timing. A switching regulator 15 rectifies the source power supply which is not illustrated, and supplies it to each part which generated and mentioned +5V and +24V above as direct current voltage as a power source.

[0023] Moreover, it consists of terminals with which a predetermined manager is performed (a personal computer, workstation, etc.), and automatic-recording management equipment 20 receives ID data of the closing motion (close leaving) time of a lock, or a transponder 18 transmitted from the wireless section 14 of the above-mentioned reader 1 in the wireless section 27, and they carry out a printout by the printer 28 in a predetermined format. In addition, in the example of illustration, a reader 1 can receive and manage in fact the information from two or more readers 1 installed in every place collectively, although there is only one.

[0024] A-2. The appearance block diagram 2 of a storage warehouse is a perspective view showing the appearance configuration of the storage warehouse where the reader mentioned above was built in. In this example, the transponder 18 is embedded in the grasping section of the existing key, and operates considering RF power signal transmitted from the reader 1 arranged in the storage warehouse as a power source. It is always or predetermined time spacing, if a reader 1 transmits RF power signal, and checks

the response from a transponder 18 and there is no response, nothing will carry out it, but if there is a response, it will attest ID data.

[0025] A-3. The block diagram 3 of a transponder (a) and (b) are the block diagrams showing the example of a configuration of a transponder 18 mentioned above. The transponder 18 shown in drawing 3 (a) consists of an antenna 19, a transceiver circuit 22, and CPU23 and EEPROM24. An antenna 19 receives RF power signal and the modulating signal which are transmitted from the reader 1 mentioned above, and supplies them to the transceiver circuit 22. It restores to an input signal, takes out the various commands transmitted from a reader 1, and supplies them to CPU23 while the transceiver circuit 22 is equipped with the rectifier circuit which is not illustrated, rectifies received RF power signal, takes out predetermined direct current voltage and supplies it to CPU23 and EEPROM24 as a power source. [0026] CPU23 builds in ROM which builds in a program, RAM as a work area, etc. (illustration abbreviation), operates with RF power signal, interprets the various commands transmitted from a reader 1, and according to the received command, various ID data beforehand stored in EEPROM24 are read, it becomes irregular by the transceiver circuit 22, and it transmits them from an antenna 19. As mentioned above, various ID data are beforehand memorized by EEPROM24, and these various ID data are suitably read to it by CPU23. Thus, when the transponder 18 shown in drawing 3 (a) is adopted, a transponder 18 transmits corresponding ID data according to ID data demand command from a reader 1.

[0027] Here, drawing 4 is the conceptual diagram showing the data format delivered and received by the above-mentioned reader 1 and the above-mentioned transponder 18. Data consist of a start bit, data (12 bits), a parity bit, and a stop bit, it is 1 character unit, and transmit various ID data by part for data division, and transmit one character of data for error checking in the same format after that so that it may illustrate. In this case, a transponder 18 transmits system discernment ID data, master key group ID data, and key ID data according to the demand from a reader 1, as shown in drawing 5. That is, if RF power is received from a reader 1, system discernment ID data will be transmitted first and automatically, and subsequently, a transponder 18 will transmit master key group ID data according to this, if a master key group ID demand command is received, and further, if a key ID-request command is received, it will transmit key ID data according to this.

[0028] In addition, system discernment ID data are set up for every manufacturer of a specially-equipped vehicle, are ID data for identifying this manufacturer, and serve as a fixed value. Moreover, grouping of the master key group ID data is carried out by the installation of a storage warehouse, and they are ID data for identifying this group, and can be changed. Furthermore, key ID data are ID data for identifying a transponder (key) 18, and can be changed too.

[0029] On the other hand, the transponder 18 shown in drawing 3 (b) consists of an antenna 19, a transceiver circuit 26, and EEPROM27. An antenna 19 receives RF power signal and the modulating signal which are transmitted from the reader 1 mentioned above, and supplies them to the transceiver circuit 26. It modulates various ID data supplied from EEPROM27, and transmits them from an antenna 19 while the transceiver circuit 26 is equipped with the rectifier circuit which is not illustrated, rectifies received RF power signal, takes out predetermined direct current voltage and supplies it to EEPROM27 as a power source. As mentioned above in EEPROM27, various ID data which various ID data were memorized beforehand, and were memorized when the power source was supplied are automatically supplied to the transceiver circuit 26. Thus, when the transponder 18 shown in drawing 3 (b) is adopted, a transponder 18 transmits various ID data beforehand memorized by EEPROM26, when RF power signal is received.

[0030] Here, drawing 6 is the conceptual diagram showing the data format delivered and received by the above-mentioned reader and the above-mentioned transponder. it illustrates -- as -- data -- a start bit (8 bits), system discernment ID data (16 bits), master key group ID data (24 bits), key ID data (24 bits), Data BCC (16 bits), and a stop bit (8 bits) -- all -- it consists of 128 bits. In this case, if a transponder 18 operates by receiving RF power as shown in drawing 7, automatically, it will be the above-mentioned data format and will transmit system discernment ID data, master key group ID data, and key ID data. In addition, the purpose of system discernment ID data, master key group ID data, and key ID data and its

contents are as having mentioned above.

[0031] A-4. Automatic-recording management equipment, next drawing 8 are the conceptual diagrams showing the configuration of the automatic-recording management equipment which totals closing motion record (close leaving record) of the lock recorded by the reader 1 mentioned above. In drawing, the wireless section 14 transmits the key ID data (is it individual or is a master?) for identifying unlocking and the time in which it was locked which were recorded as systems operation data, and the transponder (a key or card) used for unlocking and locking in a reader 1, as mentioned above. The systems operation data transmitted from the wireless section 14 are received by the wireless section 27 of the automatic-recording management equipment installed in the predetermined location.

[0032] The automatic-recording Management Department 20 consists of terminals (a personal computer, workstation, etc.) 30 with which a predetermined manager is performed, the above-mentioned wireless section 31, and a printer 32. A terminal 30 performs a predetermined manager, memorizes it to the large capacity storage (hard disk etc.) which receives by the wireless section 31 and does not illustrate the systems operation data transmitted from the wireless section 14 from two or more readers, and carries out a printout by the printer 32 in a predetermined format. In addition, when totaling if needed, a notebook computer etc. is connected to a reader 1 and you may make it manage the above-mentioned information recorded on the reader 1 through the interface of RS-232C etc.

[0033] B. Explain actuation of the transponder 18 built in the reader 1 and key which were formed in actuation of an example, next the storage warehouse by the example mentioned above. In addition, below according to the combination of the reader mentioned above, a transponder, and a data format, each actuation is explained about the following cases.

**\*\* Also explain actuation of those with CPU, those with renewal of ID functional and nothing one and CPU nothing, those with renewal of ID functional, and ID data setting processing in which it can set nothing, in having those with CPU, those with \*\*CPU with renewal of ID functional, renewal-function [ of ID ]-less \*\*CPU nothing, \*\*CPU nothing with renewal of ID functional, and no renewal function of ID, and the following.**

[0034] B-1. Unlocking / locking processing (those with \*\*CPU, those with renewal of ID functional) First, the unlocking processing at the time of using the transponder (those with renewal of ID functional) 18 equipped with CPU23 is explained. Here, drawing 9 and drawing 10 are the flow charts for [ in the reader 1 and transponder 18 in the transponder (those with renewal of ID functional) 18 equipped with CPU23 ] explaining actuation of unlocking processing.

[0035] First, at the reader 1 of a storage warehouse, RF power signal is transmitted with a predetermined time interval by the loop formation which usually consists of steps S12, S14, S16, S32, and S30 shown in drawing 9 . On the other hand, if an operator inserts a key in the keyhole 21 of a storage warehouse, the transponder 18 built in the key operates by receiving the above-mentioned RF power signal, will be step S40 shown in drawing 10 , and will read system discernment ID data, master key group ID data, and key ID data from EEPROM24. Next, system discernment ID data are transmitted in the data format shown in drawing 4 at step S42.

[0036] In a reader 1, at step S14, the above-mentioned system discernment ID data will be received, it collates with the system discernment ID data beforehand set as own EEPROM9 at step S16, and if in agreement, it will progress to step S18 and a master key group ID data demand command will be transmitted. On the other hand, at the transponder 18 of a key, if the above-mentioned master key group ID data demand command is received at step S44, it will transmit in the data format which shows the master key group ID data read at step S40 by step S46 to drawing 4 . At a reader 1, the above-mentioned master key group ID data are received at step S20. By repeating the above-mentioned steps S44 and S46, transmission and reception of a key ID data demand command and transmission and reception of key ID data are performed, and key ID data are delivered [ at the above-mentioned steps S18 and S20 and the transponder 18 of a key ] by the reader 1 of a storage warehouse and received in the data format shown in drawing 4 .

[0037] Next, at the reader 1 of a storage warehouse, if it judges whether it is in agreement by collating the above-mentioned master key group ID data and key ID data with ID data beforehand set as

EEPROM9 and is in agreement at step S22, respectively, at step S26, a random number will generate new ID data (master key group ID data or/and key ID data), and ID data of EEPROM9 will be updated and memorized. next, the step S28 -- the above -- new ID data (master key group ID data or/and key ID data) are transmitted.

[0038] on the other hand -- the transponder 18 of a key -- step S48 -- the above -- new ID data (master key group ID data or/and key ID data) -- receiving -- this -- ID data of EEPROM24 are rewritten and updated by new ID data.

[0039] Furthermore, in the reader 1 of a storage warehouse, the key ID data (is it individual or is a master?) for identifying the time which unlocked, and the transponder (a key or card) used for unlocking as systems operation data at step S30 are recorded. A reader 1 transmits the above-mentioned systems operation data periodically by the wireless section 14. It is received by the wireless section 31 of automatic-recording management equipment 20, and is totaled with a terminal 30, and the printout of these systems operation data is carried out by the printer 32 in a predetermined format.

[0040] Moreover, when not receiving any data at step S16 and the system discernment ID transmitted from the transponder 18 is not in agreement with an own thing in a reader 1, or when the master key group ID data or key ID data transmitted from the transponder 18 is not in agreement with an own thing at step S22 By step S32, after operating crime prevention and an alarm system, at step S30 mentioned above, systems operation data are recorded and it returns to step S12. Hereafter, step S12 or subsequent ones is repeated and performed.

[0041] B-2. Unlocking / locking processing (with those with \*\*CPU, and no renewal function of ID) Next, the unlocking processing at the time of using the transponder (with no renewal function of ID) 18 equipped with CPU23 is explained. Here, drawing 11 and drawing 12 are the flow charts for [ in the reader 1 and transponder 18 in the transponder (with no renewal function of ID) 18 equipped with CPU23 ] explaining actuation of unlocking processing.

[0042] First, at a reader 1, RF power signal is transmitted with a predetermined time interval by the loop formation which usually consists of steps S62, S64, S66, S78, and S76 shown in drawing 11 . On the other hand, if an operator inserts a key in the keyhole 21 of a storage warehouse, the transponder 18 built in the key operates by receiving the above-mentioned RF power signal, will be step S80 shown in drawing 12 , and will read system discernment ID data, master key group ID data, and key ID data from EEPROM24. Next, system discernment ID data are transmitted in the data format shown in drawing 4 at step S82.

[0043] In a reader 1, at step S64, the above-mentioned system discernment ID data will be received, it collates with the system discernment ID data beforehand set as own EEPROM9 at step S66, and if in agreement, it will progress to step S68 and a master key group ID data demand command will be transmitted.

[0044] On the other hand, at the transponder 18 of a key, if the above-mentioned master key group ID data demand command is received at step S84, it will transmit in the data format which shows the master key group ID data read at step S80 by step S86 to drawing 4 . At a reader 1, the above-mentioned master key group ID data are received at step S70. And key ID data are delivered [ at the above-mentioned steps S68 and S70 and the transponder 18 of a key / transmission and reception of a key ID data demand command and transmission and reception of key ID data are performed, and ] by the reader 1 of a storage warehouse, and received by repeating the above-mentioned steps S84 and S86 in the data format shown in drawing 4 .

[0045] Next, if it judges whether it is in agreement by collating the above-mentioned master key group ID data and key ID data with the data beforehand set as EEPROM9 and is in agreement in the reader 1 of a storage warehouse with step S72, respectively, the key ID data (is it individual or is a master?) for identifying the time which unlocked, and the transponder 18 used for unlocking as systems operation data at step S76 will be recorded. A reader 1 transmits the above-mentioned systems operation data periodically by the wireless section 14. It is received by the wireless section 31 of automatic-recording management equipment 20, and is totaled with a terminal 30, and the printout of these systems operation data is carried out by the printer 32 in a predetermined format.

[0046] Moreover, when not receiving any data at step S66 and the system discernment ID transmitted from the transponder 18 is not in agreement with an own thing in a reader 1, or when the master key group ID data or key ID data transmitted from the transponder 18 is not in agreement with an own thing at step S72 By step S78, after operating crime prevention and an alarm system, at step S76 mentioned above, systems operation data are recorded and it returns to step S62. Hereafter, step S62 or subsequent ones is repeated and performed.

[0047] B-3. Unlocking / locking processing (\*\*CPU nothing, those with renewal of ID functional)  
Next, the unlocking processing at the time of using the transponder (those with renewal of ID functional) 18 which is not equipped with CPU is explained. Here, drawing 13 and drawing 14 are the flow charts for [ in the reader 1 and transponder 18 in the transponder (those with renewal of ID functional) 18 which is not equipped with CPU ] explaining actuation of unlocking processing.

[0048] First, at the reader 1 of a storage warehouse, RF power signal is transmitted with a predetermined time interval by the loop formation which usually consists of steps S92, S94, S96, S106, and S104 shown in drawing 13 . On the other hand, if an operator inserts a key in the keyhole 21 of a storage warehouse, the transponder 18 built in the key operates by receiving the above-mentioned RF power signal, will be step S110 shown in drawing 14 , and will read system discernment ID data, master key group ID data, and key ID data from EEPROM27. Next, system discernment ID data master key group ID data and key ID data are transmitted in the data format shown in drawing 6 at step S112.

[0049] In a reader 1, step S94 receives the above-mentioned system discernment ID data, master key group ID data, and key ID data. At step S96 Collate with the system discernment ID data, master key group ID data, and key ID data which are beforehand set as own EEPROM9, and if in agreement, at step S100 A random number generates new ID data (master key group ID data or/and key ID data), and ID data of EEPROM9 are updated and memorized. next, the step S102 -- the above -- new ID data (master key group ID data or/and key ID data) are transmitted.

[0050] on the other hand -- the transponder 18 of a key -- step S114 -- the above -- new ID data (master key group ID data or/and key ID data) -- receiving -- step S116 -- this -- ID data of EEPROM27 are rewritten and updated by new ID data.

[0051] Furthermore, in the reader 1 of a storage warehouse, the key ID data (is it individual or is a master?) for identifying the time which unlocked, and the transponder 18 used for unlocking as systems operation data at step S104 are recorded. A reader 1 transmits the above-mentioned systems operation data periodically by the wireless section 14. It is received by the wireless section 31 of automatic-recording management equipment 20, and is totaled with a terminal 30, and the printout of these systems operation data is carried out by the printer 32 in a predetermined format.

[0052] Moreover, in a reader 1, when at least one of the system discernment ID transmitted from the transponder 18 when any data were not received at step S96, master key group ID data, or the key ID data is not in agreement with an own thing, after operating crime prevention and an alarm system, at step S104 mentioned above, systems operation data are recorded and it returns to step S92 by step S106. Hereafter, step S92 or subsequent ones is repeated and performed.

[0053] B-4. Unlocking / locking processing (with \*\*CPU nothing and no renewal function of ID)  
Next, the unlocking processing at the time of using the transponder (with no renewal function of ID) 18 which is not equipped with CPU is explained. Here, drawing 15 and drawing 16 are the flow charts for [ in the reader 1 and transponder 18 in the transponder (with no renewal function of ID) 18 which is not equipped with CPU ] explaining actuation of unlocking processing.

[0054] First, at the reader 1 of a storage warehouse, RF power signal is transmitted with a predetermined time interval by the loop formation which usually consists of steps S122, S124, S126, S132, and S130 shown in drawing 15 . On the other hand, if an operator inserts a key in the keyhole 21 of a storage warehouse, the transponder 18 built in the key operates by receiving the above-mentioned RF power signal, will be step S140 shown in drawing 16 , and will read system discernment ID data, master key group ID data, and key ID data from EEPROM27. Next, system discernment ID data master key group ID data and key ID data are transmitted in the data format shown in drawing 6 at step S142.

[0055] In a reader 1, step S124 receives the above-mentioned system discernment ID data, master key

group ID data, and key ID data. At step S126 Collate with the system discernment ID data, master key group ID data, and key ID data which are beforehand set as own EEPROM9, and if in agreement, at step S130 The key ID data (is it individual or is a master?) for identifying the time which unlocked, and the transponder (a key or card) 18 used for unlocking as systems operation data are recorded. A reader 1 transmits the above-mentioned systems operation data periodically by the wireless section 25. It is received by the wireless section 31 of automatic-recording management equipment 20, and is totaled with a terminal 30, and the printout of these systems operation data is carried out by the printer 32 in a predetermined format.

[0056] Moreover, in a reader 1, when at least one of the system discernment ID transmitted from the transponder 18 at step S126, master key group ID data, or the key ID data is not in agreement with an own thing, after operating crime prevention and an alarm system, at step S130 mentioned above, systems operation data are recorded and it returns to step S122 by step S132. Hereafter, step S122 or subsequent ones is repeated and performed.

[0057] Thus, in unlocking / locking processing, when an operator inserts a key in the keyhole 21 of a storage warehouse, the transponder 18 built in the key is receiving RF power from a reader 1, and will transmit ID data automatically. And if ID data are in agreement, the time at that time and ID data of a transponder 18 will be recorded. And it is received by the wireless section 31 of automatic-recording management equipment 20 to predetermined timing, and is totaled with a terminal 30, and the printout of the recorded this information is carried out by the printer 32 in a predetermined format. Therefore, the time of unlocking and locking of a storage warehouse and the transponder 18 then used are automatically manageable. Moreover, not a storage warehouse but the room, then close leaving are automatically manageable.

[0058] B-5. ID data setting processing (those with CPU)

Next, ID data setting processing at the time of using the transponder 18 equipped with CPU23 is explained. At the time of shipment of a reader 1 and a transponder 18, the ID data setting processing concerned is performed, when changing ID data (master key group ID data or/and key ID data) already set as the reader 1 and the transponder 18 in loss of a key etc. here, drawing 17 thru/or drawing 19 are the flow charts for explaining actuation of ID data setting processing in a setter (illustration abbreviation), a reader 1, and a transponder 18 in the transponder (- with renewal of ID functional -- nothing) 18 equipped with CPU23.

[0059] In the setter which is not illustrated, first, at step S150, new ID data (master key group ID data or/and key ID data) are set up, and it is moved to data communication within the limits of a reader 1. And if it moves to data communication within the limits of a reader 1, system discernment ID data will be transmitted to the reader 1 of a storage warehouse at step S152.

[0060] On the other hand, in the reader 1 of a storage warehouse, when a setter moves to communication link within the limits of this reader, in step S160 shown in drawing 18, the data (system discernment ID) transmitted from a setter are received automatically. Next, if data are received, it will collate whether it is in agreement with the system discernment ID from which the received data are beforehand set as EEPROM9 at step S162, and if in agreement, it will progress to step S164 and a master key group ID data demand command will be transmitted to a setter.

[0061] When a master key group ID data demand command is received from a reader 1, in a setter, at step S154 at step S156 the command of setting up new ID data (master key group ID data or/and key ID data) -- in other words After transmitting to the reader 1 of a storage warehouse, predetermined data other than the master key group ID data to a master key group ID data demand command at step S158 New ID data (master key group ID data or/and key ID data) are transmitted to a reader 1.

[0062] In the reader 1 of a storage warehouse, the data to a master key group ID data demand are received at step S166, and it judges whether the data received at step S168 are setting data (command) of new ID data, and progresses that it is setting data to step S170, and new ID data (master key group ID data or/and key ID data) transmitted from the setter are received. Next, ID data stored in EEPROM9 are updated and memorized at step S172 with received new ID data (master key group ID data or/and key ID data). and the step S174 -- the transponder 18 of a key -- receiving -- the above -- new ID data



(master key group ID data or/and key ID data) are transmitted.

[0063] On the other hand, at the transponder 18 of a key, if the transponder 18 concerned is in the data communication range of a reader, by step S190 shown in drawing 19, new ID data will be received automatically, and ID data stored in EEPROM24 will be updated and memorized by new ID data (master key group ID data or/and key ID data) received at step S192.

[0064] On the other hand, at a reader 1, modification of new ID data (master key group ID data or/and key ID data) is checked by delivering and receiving ID data between the transponders 18 of a key as completion processing of ID data modification of a system at step S176 shown in drawing 18. And it records having changed the key ID data (is it individual or is a master?) and ID data for identifying the time and the transponder (key) 18 which changed ID data (setup) as systems operation data at step S178 (setup). A reader 1 transmits the above-mentioned systems operation data periodically by the wireless section 14. It is received by the wireless section 31 of automatic-recording management equipment 20, and is totaled with a terminal 30, and the printout of these systems operation data is carried out by the printer 32 in a predetermined format.

[0065] Moreover, in the reader 1 of a storage warehouse, when the system discernment ID and the own system discernment ID which were transmitted from the setter at step S162 are not in agreement, or when the data received at step S168 are not setting data (command) of new ID data, crime prevention and an alarm system are operated at step S180.

[0066] Thus, in using the transponder 18 equipped with CPU23 according to the processing mentioned above, in case it sets up new ID data, while transmitting system ID data to the reader 1 of a storage warehouse, this reader 1 can be made to shift to new ID data reception automatically by transmitting predetermined data to the master key group ID data demand command from a reader 1. Therefore, a reader 1 and a transponder 18 can set up new ID data (master key group ID data or/and key ID data) by performing the usual data transfer processing and same data transfer processing.

[0067] B-6. ID data setting processing (with no CPU)

Next, ID data setting processing at the time of using the transponder 18 which is not equipped with CPU is explained. here, drawing 20 thru/or drawing 22 are the flow charts for explaining actuation of ID data setting processing in a setter (illustration abbreviation), a reader 1, and a transponder 18 in the transponder (- with renewal of ID functional -- nothing) 18 which is not equipped with CPU.

[0068] At the setter which is not illustrated, first, at step S200 shown in drawing 20, new ID data (master key group ID data or/and key ID data) are set up, and it is moved to data communication within the limits of a reader 1. And if it moves to data communication within the limits of a reader 1, after transmitting the setter ID data for identifying a setter to the reader 1 of a storage warehouse at step S202, new ID data are transmitted at step S204.

[0069] On the other hand, in the reader 1 of a storage warehouse, when a setter moves to communication link within the limits, in step S210 shown in drawing 21, the setter ID data transmitted from a setter are received automatically. Next, reception of setter ID data receives whether the received setter ID data are predetermined data and new ID data which progresses to step S214 and is transmitted from a setter when it collates and is predetermined data at step S212.

[0070] Next, a reader 1 is step S216, and updates and memorizes ID data stored in EEPROM9 by received new ID data (master key group ID data or/and key ID data). and the step S218 -- the transponder 18 of a key -- receiving -- the above -- new ID data (master key group ID data or/and key ID data) are transmitted.

[0071] On the other hand, at the transponder 18 of a key, if the transponder 18 concerned is in the data communication range of a reader 1, by step S230 shown in drawing 22, new ID data will be received automatically, and ID data stored in EEPROM27 will be updated and memorized by new ID data (master key group ID data or/and key ID data) received at step S232.

[0072] On the other hand, at a reader 1, modification of new ID data (master key group ID data or/and key ID data) is checked by delivering and receiving ID data between the transponders 18 of a key as completion processing of ID data modification of a system at step S220 shown in drawing 21. And it records having changed the key ID data (is it individual or is a master?) and ID data for identifying the



time and the transponder (key) 18 which changed ID data (setup) as systems operation data at step S222 (setup). A reader 1 transmits the above-mentioned systems operation data periodically by the wireless section 14. It is received by the wireless section 31 of automatic-recording management equipment 20, and is totaled with a terminal 30, and the printout of these systems operation data is carried out by the printer 32 in a predetermined format.

[0073] Moreover, in the reader 1 of a storage warehouse, when the setter ID data transmitted from the setter at step S212 are not predetermined data, crime prevention and an alarm system are operated at step S224.

[0074] Thus, when using the transponder 18 which is not equipped with CPU23 according to the processing mentioned above, in case new ID data are set up, this reader 1 can be made to shift to new ID data reception automatically by transmitting the setter ID data of a setter proper to the reader 1 of a storage warehouse. Therefore, a reader 1 and a transponder 18 can set up new ID data (master key group ID data or/and key ID data) by performing the usual data transfer processing and same data transfer processing.

[0075] In addition, although one key which contained the transponder 18 explained the storage warehouse which unlocks a lock in the above-mentioned example, in order to raise safety more, when two or more keys are assembled, you may be the storage warehouse which unlocks a lock. In this case, what is necessary is just to emit an alarm, if the transponder 18 of each key is made to memorize different ID data and two or more above-mentioned ID data of not all are in agreement in a reader 1 side. moreover -- although it was made to operate crime prevention and an alarm system when ID data of the transponder 18 of a key and the reader 1 of a storage warehouse were inharmonious -- specifically reporting through a communication line in operating a security camera \*\*\*\* [ and ] \*\*\*\* -- as -- you may make it use combining at least one or these [ sounding an alarm tone ] Furthermore, although information was delivered and received by wireless between a reader 1 and automatic-recording management equipment 20, you may make it transmit not only through this but through a cable or the telephone line in the above-mentioned example.

[0076] Moreover, although use of the key which does not contain a transponder 18 is not taken into consideration in the above-mentioned example, as shown in drawing 1 By forming the microswitch 33 which detects closing motion of the door of a storage warehouse through PIO12 When it is unlocked/locked and a door is opened and closed with the key which does not contain a transponder 18, closing motion of a door is detected with the above-mentioned microswitch 33, and you may make it memorize the time at that time etc. Even if it is the case where this uses the key which does not contain the transponder 18, close leaving, a maintenance, etc. are easily manageable. Furthermore, when the key which does not contain a transponder 18 is used, while judging that it is an unauthorized use and operating crime prevention and an alarm system, it may be made to record the above-mentioned time etc.

[0077]

[Effect of the Invention] If answerback approaches a storage warehouse according to invention according to claim 1, the high-frequency field from the RF generating means of a reader will be made into power. If the response device identification data with which the response device identification data memorized by the 1st storage means from the 1st transmitting means are transmitted, and these response device identification data are memorized by the 2nd storage means of a reader are in agreement a record means -- a time check -- since the current time by the means was recorded, the advantage that close leaving, a maintenance, etc. are easily manageable is acquired by grasping the closing motion of a lock produced at the time of close leaving or a maintenance.

[0078] Moreover, since warning was emitted with the warning means when the response device identification data memorized by the response device identification data received by said 1st receiving means and said 2nd storage means were not in agreement according to invention according to claim 2, the advantage that confidentiality can be raised more and safety can be raised more is acquired.

[0079] Moreover, according to invention according to claim 3, by said RF generating means, with a predetermined time interval, since it was made to generate a high-frequency field, the advantage that

power consumption can be reduced is acquired.

[0080] Moreover, according to invention according to claim 4, since said answerback and said reader delivered and received the master key group discernment data which identify the installation area of the system discernment data which identify a system, and a storage warehouse in addition to said response device identification data, the advantage that close leaving, a maintenance, etc. can be managed easily and more strictly is acquired by grasping the closing motion of a lock produced at the time of close leaving or a maintenance.

[0081] According to invention according to claim 5, a predetermined communications protocol is followed and said answerback is equipped with the 2nd control means which controls the data transfer between said readers. Moreover, between said answerbacks and said readers Since said system discernment data, said master key group discernment data, and said response device identification data were delivered and received according to said predetermined communications protocol The advantage that close leaving, a maintenance, etc. can be managed easily and more strictly is acquired by grasping the closing motion of a lock produced at the time of close leaving or a maintenance.

[0082] Moreover, since response device identification data required for authentication whenever it unlocks an electric lock were rewritten according to invention according to claim 6, the advantage that the unjust copy of answerback can both be prevented as if confidentiality can be raised more and safety can be raised more is acquired.

[0083] Moreover, the advantage that it can update is acquired, without exchanging hardware, since rewriting of discernment data can be performed in non-contact even when loss of answerback (key) and a theft arise according to invention according to claim 7, since it was made to enable rewriting of said response device identification data and master key group discernment data by radio with an external setting device.

[0084] According to invention claim 8 thru/or given in 11, the information memorized by the account record means of a reading means moreover, with an output means Since it sends out to an external instrument through wireless, a cable, or the telephone line, a receiving means receives the information outputted from said output means in the management tool formed as an external instrument and the this received information was totaled with the total means The advantage that close leaving, a maintenance, etc. can be managed easily and more strictly is acquired by grasping the closing motion of a lock produced at the time of close leaving or a maintenance.

[0085] Moreover, when according to invention according to claim 12 it is unlocked/locked and a door is opened and closed with the key which does not contain answerback with a detection means since closing motion of a door was detected, closing motion of a door is detected with the above-mentioned detection means, and you may make it memorize the time at that time etc. Even if it is the case where this uses the key which does not contain answerback, the advantage that close leaving, a maintenance, etc. are easily manageable is acquired.

---

[Translation done.]

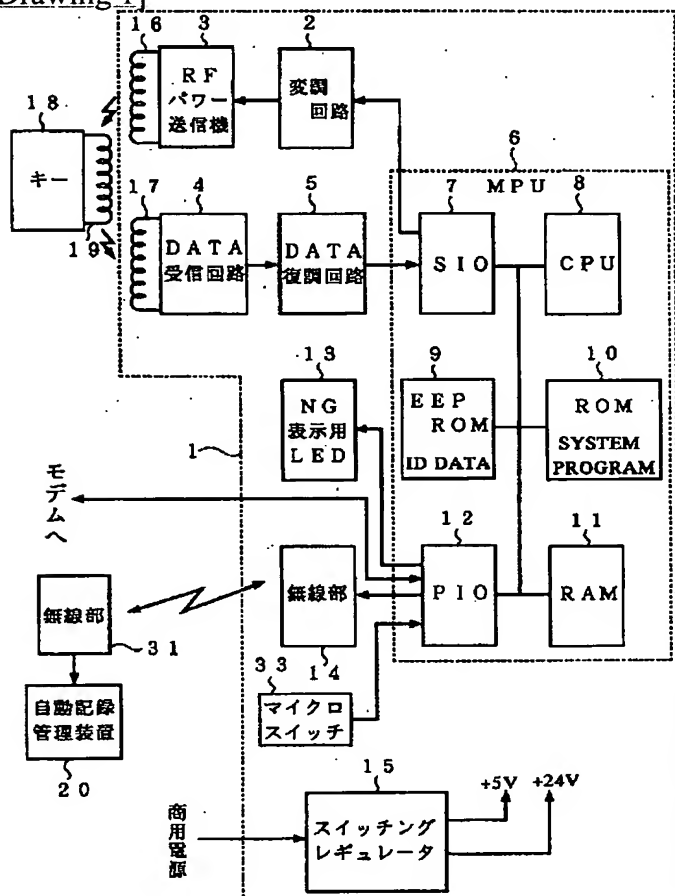
## \* NOTICES \*

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

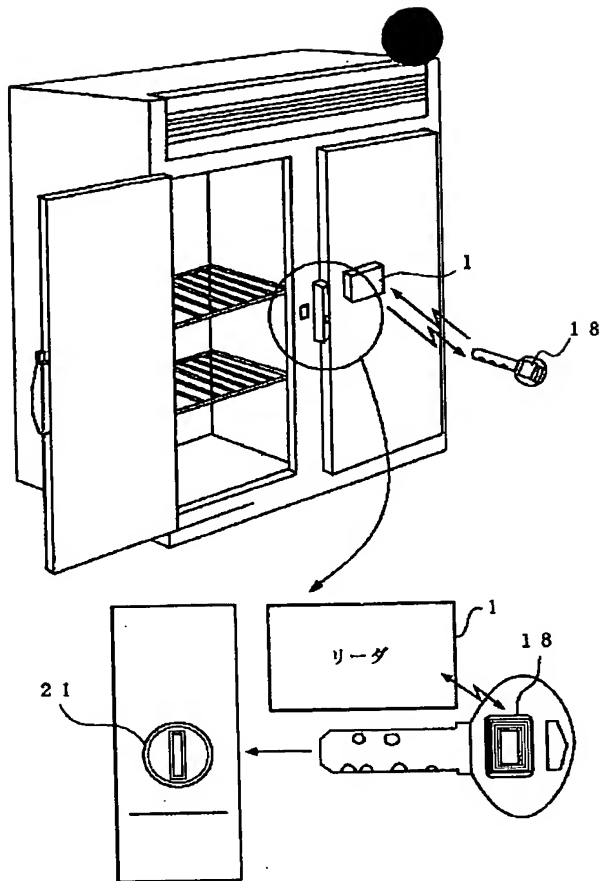
1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

## DRAWINGS

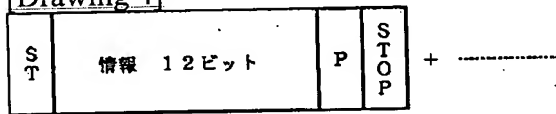
[Drawing 1]



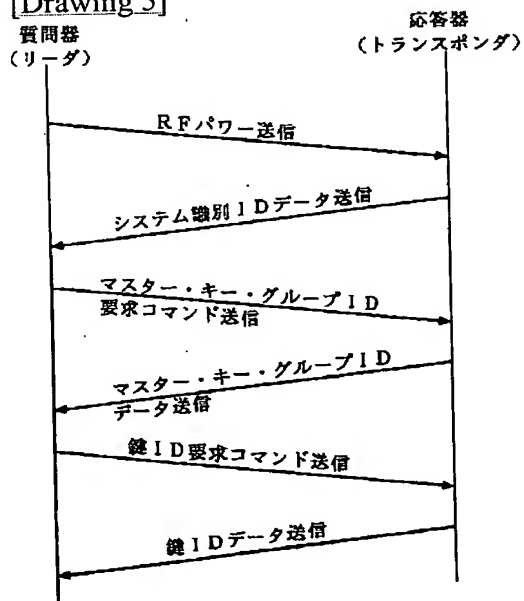
[Drawing 2]



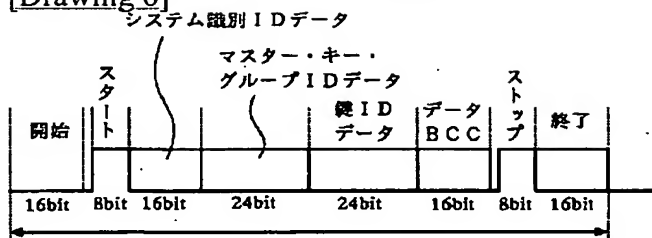
[Drawing 4]



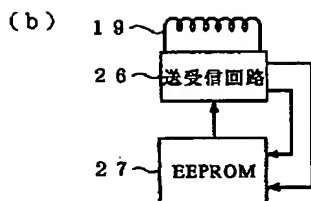
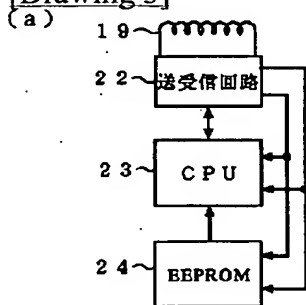
[Drawing 5]



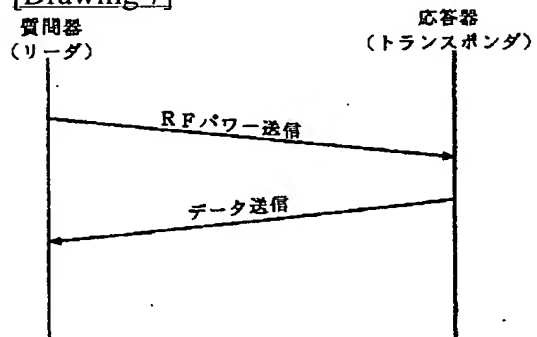
[Drawing 6]



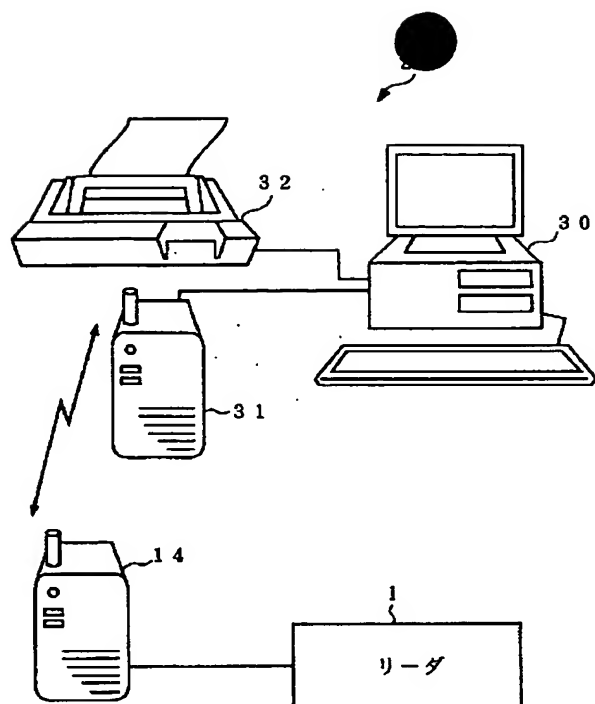
[Drawing 3]



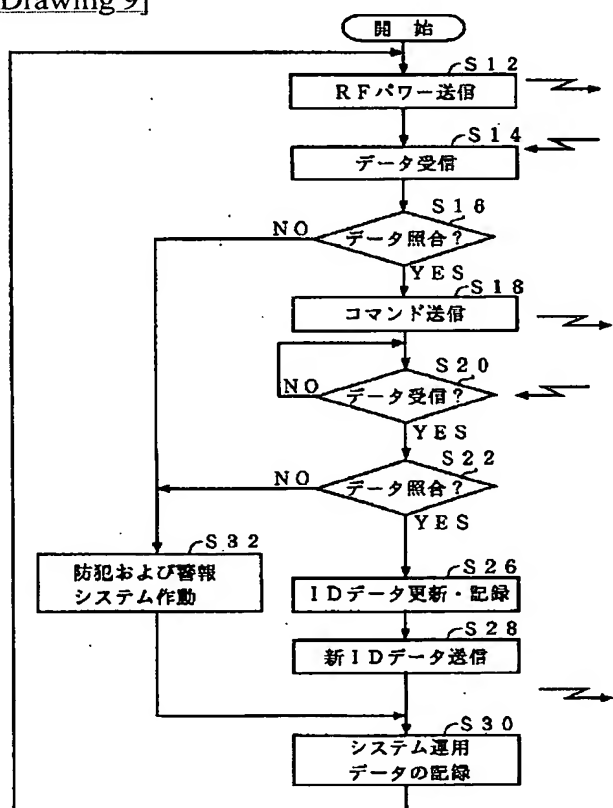
[Drawing 7]



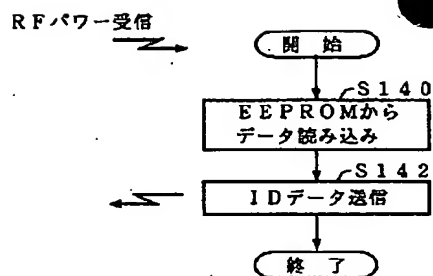
[Drawing 8]



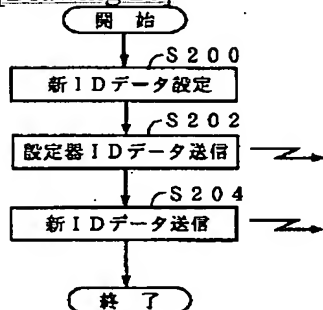
[Drawing 9]



[Drawing 16]

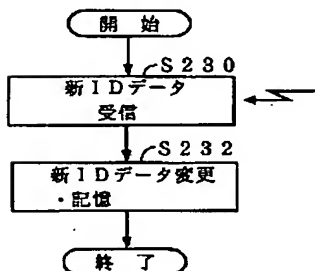


[Drawing 20]

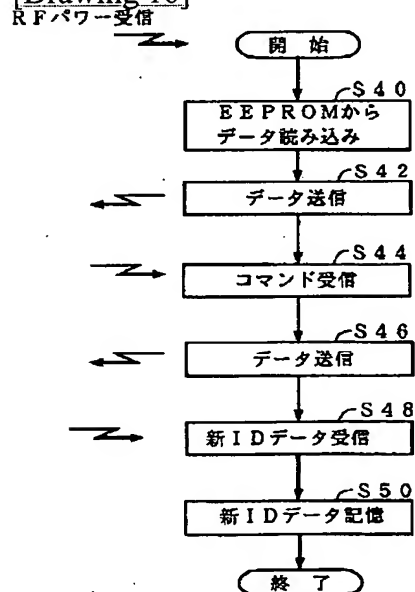


[Drawing 22]

IDデータ設定時のトランスポンダ

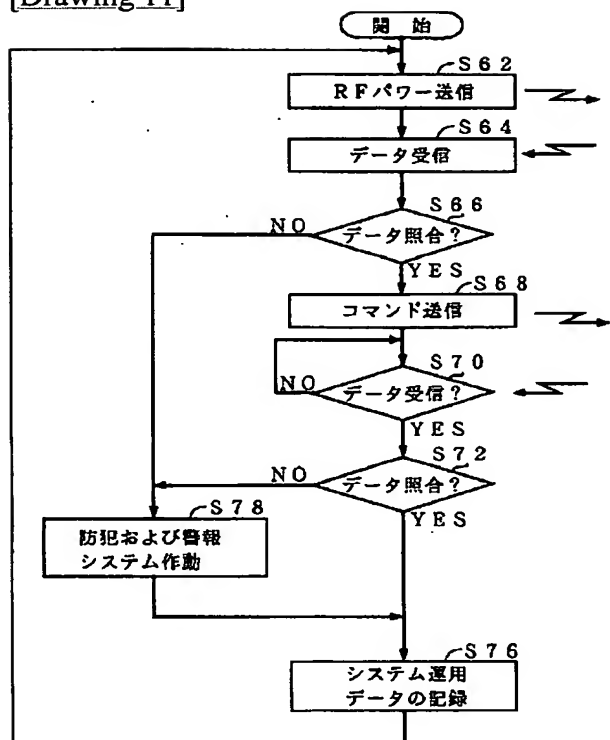


[Drawing 10]

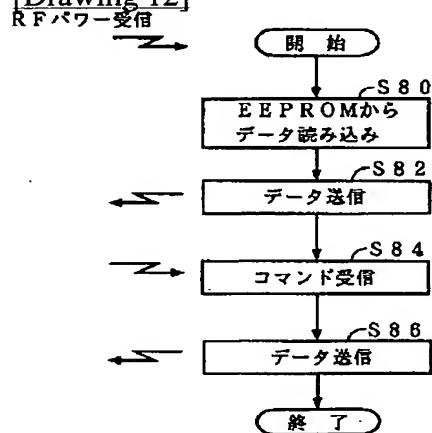




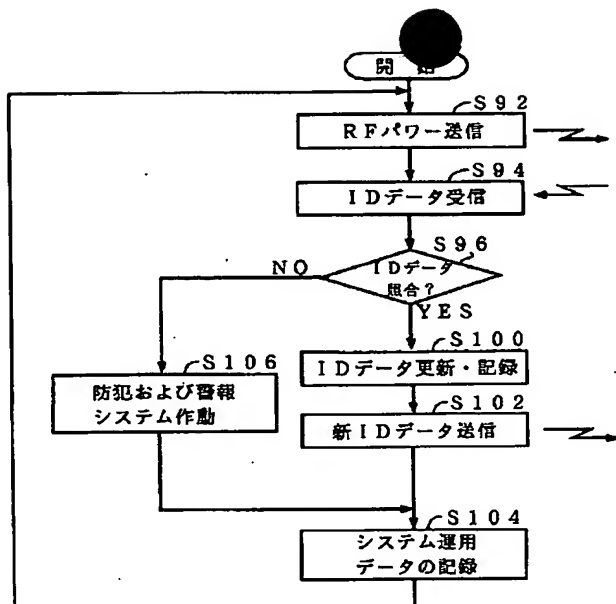
[Drawing 11]



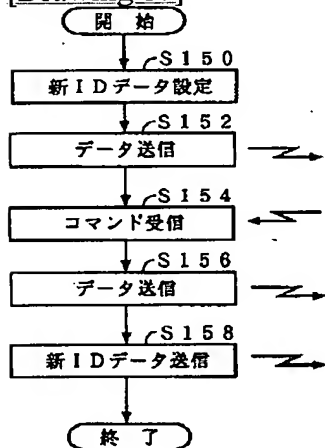
[Drawing 12]



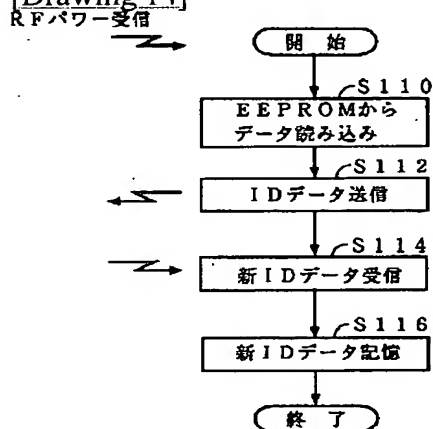
[Drawing 13]



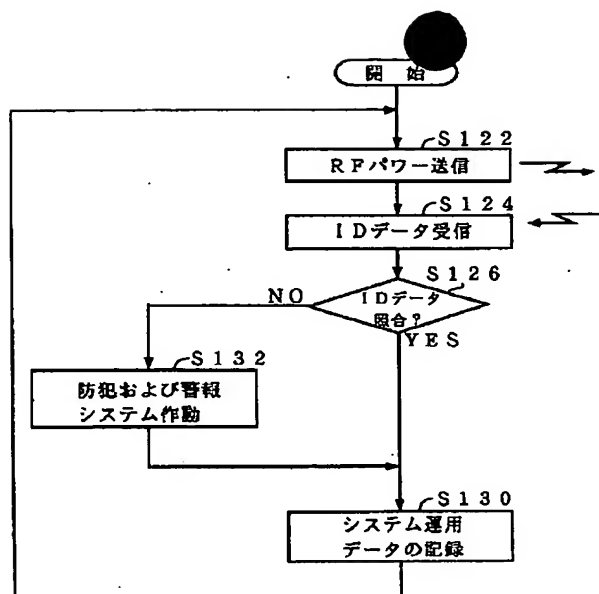
[Drawing 17]



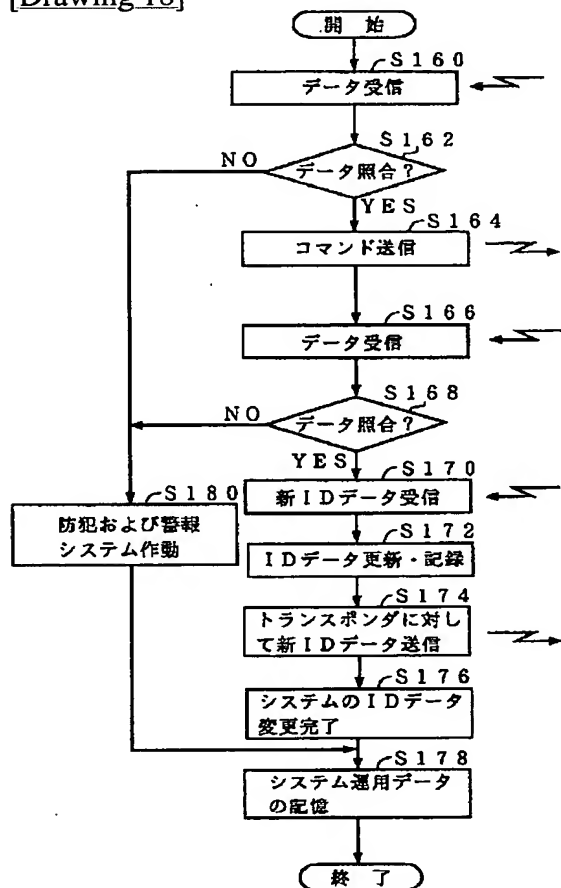
[Drawing 14]



[Drawing 15]

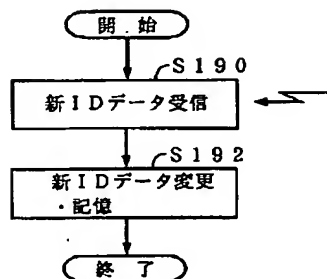


[Drawing 18]

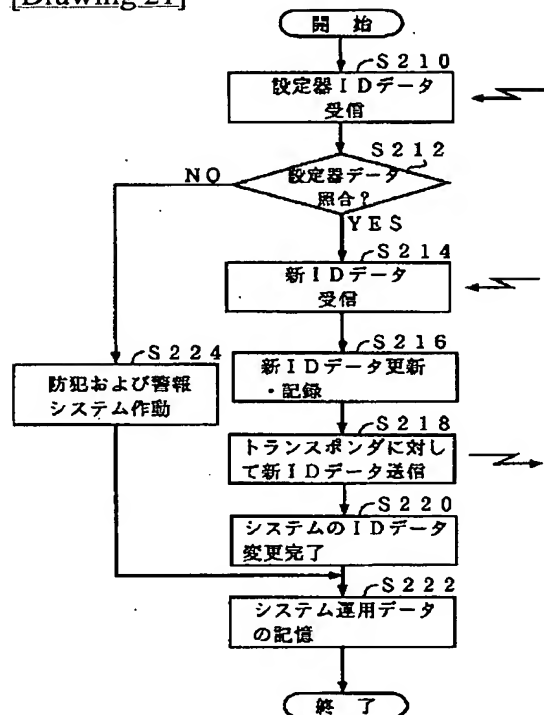


[Drawing 19]

## IDデータ設定時のトランスポンダ



[Drawing 21]



[Translation done.]

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**